THE CYBER TALENT PIPELINE: EDUCATING A WORKFORCE TO MATCH TODAY'S THREATS

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

JULY 29, 2021

Serial No. 117–27

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

46–039 PDF WASHINGTON : 2021

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
DONALD M. PAYNE, JR., New Jersey
J. LUIS CORREA, California
ELISSA SLOTKIN, Michigan
EMANUEL CLEAVER, Missouri
AL GREEN, Texas
YVETTE D. CLARKE, New York
ERIC SWALWELL, California
DINA TITUS, Nevada
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
VAL BUTLER DEMINGS, Florida
NANETTE DIAZ BARRAGÁN, California
JOSH GOTTHEIMER, New Jersey
ELAINE G. LURIA, Virginia
TOM MALINOWSKI, New Jersey
RITCHIE TORRES, New York
JOHN KATKO, New York
MICHAEL T. MCCAUL, Texas
CLAY HIGGINS, Louisiana
MICHAEL GUEST, Mississippi
DAN BISHOP, North Carolina
JEFFERSON VAN DREW, New Jersey
RALPH NORMAN, South Carolina
MARIANNETTE MILLER-MEEKS, Iowa
DIANA HARSHBARGER, Tennessee
ANDREW S. CLYDE, Georgia
CARLOS A. GIMENEZ, Florida
JAKE LATURNER, Kansas
PETER MEIJER, Michigan
KAT CAMMACK, Florida
AUGUST PFLUGER, Texas
ANDREW R. GARBARINO, New York

HOPE GOINS, *Staff Director*
DANIEL KROESE, *Minority Staff Director*
NATALIE NIXON, *Clerk*

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

YVETTE D. CLARKE, New York, *Chairwoman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
ELISSA SLOTKIN, Michigan
KATHLEEN M. RICE, New York
RITCHIE TORRES, New York
BENNIE G. THOMPSON, Mississippi *(ex officio)*
ANDREW R. GARBARINO, New York, *Ranking Member*
RALPH NORMAN, South Carolina
DIANA HARSHBARGER, Tennessee
ANDREW CLYDE, Georgia
JAKE LATURNER, Kansas
JOHN KATKO, New York *(ex officio)*

MOIRA BERGIN, *Subcommittee Staff Director*
AUSTIN AGRELLA, *Minority Subcommittee Staff Director*
MARIAH HARDING, *Subcommittee Clerk*

CONTENTS

THE CYBER TALENT PIPELINE: EDUCATING A WORKFORCE TO MATCH TODAY'S THREATS

Thursday, July 29, 2021

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY,
INFRASTRUCTURE PROTECTION,
AND INNOVATION,
Washington, DC.

The subcommittee met, pursuant to notice, at 10 a.m., via Webex, Hon. Yvette D. Clarke [Chairwoman of the subcommittee] presiding.

Present: Representatives Clarke, Langevin, Slotkin, Rice, Torres, Garbarino, Harshbarger, and Clyde.

Chairwoman CLARKE. The Subcommittee on Cybersecurity Infrastructure Protection and Innovation will come to order.

Without objection, the Chair is authorized to declare the subcommittee in recess at any point.

Good morning and thank you to our witnesses for joining us today for this hearing on strengthening our Nation's cybersecurity work force.

A recent report by the cybersecurity firm Sonicwall found that ransomware attacks in North America increased 158 percent between 2019 and 2020. Another report by Comparitech found that cyber attacks against U.S. Government organizations affected 71 million Americans and cost over $18 billion in down time and recovery.

The surge in cyber attacks against State and local governments, hospitals, and school districts, coupled with recent headlines about SolarWinds, Colonial Pipeline, and Kaseya have galvanized new calls to action to better defend the internet ecosystem. I am encouraged by the momentum, and I am committed to putting more resources in the hands of State and local governments and improving CISA's awareness of malicious cyber activity through cyber incident reporting.

But without a capable cyber work force, all of our investments in tools and data will be in vain. The number of high-profile cyber incidents over the past year has emphasized just how essential cybersecurity has become. The truth is the number of trained cybersecurity professionals has not increased to the levels necessary to meet the demand from industry and Government. In fact, recent data show a deficit of over 460,000 trained cybersecurity professionals in the United States, relative to our current needs.

While the Federal Government has undertaken several initiatives in recent years to expand and better train our Nation's cybersecurity work force, we must do more. This hearing will give us an opportunity to hear from experts in the field who are working to educate the next generation of cybersecurity workers, so we can learn more about the programs that are currently in place and where greater investment is needed. There is no silver bullet. We will need a multi-pronged approach that focuses on training the cybersecurity work force of the future in schools and universities, reskilling existing workers for the jobs that are currently available, and making sure we have the right training in place to address the disparate cybersecurity challenges in information technology and operational technology.

During my 15 years in Congress working on cybersecurity issues, I have heard consistently about the importance of prioritizing K–12 cyber education to grow and diversify the talent pipeline. Over that time, an entire generation of students has graduated high school and entered higher education or the work force, and we still are behind where we need to be in including cyber education at the elementary and secondary level. However, CISA's Cybersecurity Education and Training Assistance Program, CETAP, has begun to show meaningful results. I am glad Congress demonstrated support for CETAP by formally authorizing the program in last year's National Defense Authorization Act, and it is essential that Congress continues to provide it with the resources necessary to carry out its mission.

I look forward to hearing today from the CETAP grant recipient, cyber.org, to learn more about their progress in developing curriculums for K–12 educators and what more can be done to both expand resources to teachers and build awareness of existing programs. Reaching children in the K–12 environment is an important step in making sure we don't leave talent untapped. Just as important, however, is that we reach students in college, contemplating college, or mid-career who may not have considered a career in cybersecurity to be a viable option. That is is where bringing cybersecurity work force programs to overlooked communities and reskilling programs come in, and I look forward to hearing from California State University at San Bernardino on its important work in this space.

Finally, as we look for new opportunities to redouble our efforts to grow our Nation's cyber talent, I want to be mindful that cybersecurity training is not one size fits all. The recent Colonial Pipeline ransomware attack highlighted the significant impact any incident involving critical infrastructure can have. While the attack only affected the information technology systems of the pipeline company, the precautionary decision to shut off operational technology systems reflected the vulnerability of our industrial control systems.

As we work to address our cyber work force shortage, we must remain cognizant of the different skills and positions involved in securing industrial control systems and ensure that our training programs fully reflect the broad range of cybersecurity threats we face.

Before I close, I want to commend Secretary Mayorkas for making enhancing the cyber work force the second of DHS's 60-day cyber sprints. By prioritizing this aggressive approach, Secretary Mayorkas has made meaningful progress in reducing the significant number of cyber vacancies at the Department while taking additional steps to address the shortage of cyber professionals nationally. A diverse and skilled work force has always been a competitive advantage for our Nation against our adversaries, but with constantly evolving cyber threats, we must continuously be looking to enhance our cyber education to stay ahead.

I look forward to the testimony of our witnesses and the discussion today so this subcommittee can continue working to enhance our Nation's cyber work force.

[The statement of Chairwoman Clarke follows:]

STATEMENT OF CHAIRWOMAN YVETTE D. CLARKE

JULY 29, 2021

A recent report by the cybersecurity firm Sonicwall found that ransomware attacks in North America increased 158 percent between 2019 and 2020. Another report by Comparitech found that cyber attacks against U.S. Government organizations affected 71 million Americans and cost over $18 billion in downtime and recovery. The surge in cyber attacks against State and local governments, hospitals, and school districts, coupled with recent headlines about SolarWinds, Colonial Pipeline, and Kaseya have galvanized new calls to action to better defend the internet ecosystem.

I am encouraged by the momentum, and I am committed to putting more resources in the hands of State and local governments and improving CISA's awareness of malicious cyber activity through cyber incident reporting. But without a capable cyber workforce, all of our investments in tools and data will be in vain. The number of high-profile cyber incidents over the past year has emphasized just how essential cybersecurity has become. And the truth is the number of trained cybersecurity professionals has not increased to the levels necessary to meet the demand from industry and Government. In fact, recent data show a deficit of over 460,000 trained cybersecurity professionals in the United States, relative to our current needs.

While the Federal Government has undertaken several initiatives in recent years to expand and better train our Nation's cybersecurity workforce, we must do more. This hearing will give us an opportunity to hear from experts in the field who are working to educate the next generation of cybersecurity workers, so we can learn more about the programs that are currently in place and where greater investment is needed.

There is no silver bullet. We will need a multi-pronged approach that focuses on training the cybersecurity workforce of the future in schools and universities, reskilling existing workers for the jobs that are currently available, and making sure we have the right training in place to address the disparate cybersecurity challenges in Information Technology and Operational Technology.

During my 15 years in Congress working on cybersecurity issues, I have heard consistently about the importance of prioritizing K–12 cyber education to grow and diversify the talent pipeline. Over that time, an entire generation of students has graduated high school and entered higher education or the workforce, and we still are behind where we need to be in including cyber education at the elementary and secondary level. However, CISA's Cybersecurity Education and Training Assistance Program, or CETAP has begun to show meaningful results.

I am glad Congress demonstrated support for CETAP by formally authorizing the program in last year's National Defense Authorization Act, and it is essential that Congress continues to provide it with the resources necessary to carry out its mission. I look forward to hearing today from the CETAP grant recipient, CYBER.ORG, to learn more about their progress in developing curriculums for K–12 educators and what more can be done to both expand resources to teachers and build awareness of existing programs. Reaching children in the K–12 environment is an important step in making sure we don't leave talent untapped.

Just as important, however, is that we reach students in college, contemplating college, or mid-career who may not have considered a career in cybersecurity to be

a viable option. That is where bringing cybersecurity workforce programs to overlooked communities and reskilling programs come in, and I look forward to hearing from California State University, San Bernardino on its important work in this space.

Finally, as we look for new opportunities to redouble our efforts to grow our Nation's cyber talent, I want to be mindful that cybersecurity training is not one size fits all. The recent Colonial Pipeline ransomware attack highlighted the significant impact any incident involving critical infrastructure can have. While the attack only affected the information technology systems of the pipeline company, the precautionary decision to shut off operational technology systems reflected the vulnerability of our industrial control systems. As we work to address our cyber workforce shortage, we must remain cognizant of the different skills and positions involved in securing industrial control systems and ensure that our training programs fully reflect the broad range of cybersecurity threats we face.

Before I close, I want to commend Secretary Mayorkas for making enhancing the cyber workforce the second of DHS's 60-day cyber sprints. By prioritizing this aggressive approach, Secretary Mayorkas has made meaningful progress in reducing the significant number of cyber vacancies at the Department while taking additional steps to address the shortage of cyber professionals Nationally. A diverse and skilled workforce has always been a competitive advantage for our Nation against our adversaries, but with constantly-evolving cyber threats, we must continuously be looking to enhance our cyber education to stay ahead.

Chairwoman CLARKE. The Chair now recognizes the Ranking Member of the subcommittee, the gentleman from New York, Mr. Garbarino, for an opening statement.

Mr. GARBARINO. Thank you, Chairwoman. Thank you very much. This is a great hearing. Thank you for holding this critical conversation regarding our cyber talent pipeline and our shared efforts to develop a robust cyber work force.

I would like to thank our witnesses for being here today. I look forward to a constructive dialog on this important issue.

Is it not working?

Chairwoman CLARKE. Mr. Garbarino, I think for some reason we are not hearing you. Try unmuting once again. We still aren't hearing you.

Ms. SLOTKIN. Madam Chair? I could hear him the first time. I heard him loud and——

Mr. GARBARINO. Can you hear me now?

Ms. SLOTKIN. I can.

Mr. GARBARINO. It worked? So now it is working? OK. Thank you.

All right. Thank you, Madam Chair, for holding this critical conversation regarding our cyber talent pipeline and our shared efforts to develop a robust cyber work force.

I would like to thank our witnesses for being here today. I look forward to a constructive dialog on this important issue.

Everyone in this hearing should understand the multitude of issues contributing to our cyber work force shortage, which is particularly acute in the Federal sector. Lack of exposure, uneven education, and issues with Federal agency on-boarding all contribute to the problem. Fortunately, President Biden's choices for the top three cyber professionals in the administration are real professionals and there is a wealth of private and Federal sector experience among them. I am confident that Jen Easterly, Anne Neuberger, and Chris Inglis will have the experience, the talent, and drive to address the issue, as well as the many others facing our Nation in the space.

The administration's work has already been seen in CISA's deployment of Stopransomware.gov, the U.S. Government's official one-stop location for resources to tackle ransomware more effectively.

But their work is not done. CISA has been plagued by hiring delays, elongated on-boarding processes, a lack of professional human resources specialists, and duplicative and arbitrarily onerous vetting requirements. It is important that we continue to hold CISA and the Department accountable when it comes to these troubling issues. I appreciate the Chairwoman working with me on our oversight of the cyber talent management system roll-out. I am pleased that CISA director Jen Easterly has said this will be a top priority during her tenure.

Our concerns are particularly relevant to today's hearing because no matter how much education we provide to our students, no matter how much interest we cultivate, none of it matters if we can't bring qualified and interested individuals into the Government service in a professional and timely manner. Quite simply, we will continue shouting into the wind until we fix these issues.

I look forward to exploring all these issues with our witnesses today and I hope to hear about concrete proposals for oversight in legislation, not just broad stroke ideas, which have been the output of similar hearings in the past and have proven ineffective.

Again, I thank the Chairwoman for holding this timely and important hearing today.

Thank you.

[The statement of Ranking Member Garbarino follows:]

STATEMENT OF RANKING MEMBER ANDREW R. GARBARINO

Thank you, Madam Chair, for holding this critical conversation regarding our cyber talent pipeline and our shared efforts to develop a robust cyber workforce. I'd like to thank our witnesses for being here today. I look forward to a constructive dialog on this important issue.

Everyone in this hearing should understand the multitude of issues contributing to our cyber workforce shortage, which is particularly acute in the Federal sector. Lack of exposure, uneven education, and Federal agency on-boarding issues all contribute to the problem.

Fortunately, President Biden's choices for the top three cyber professionals in the administration are real professionals, and there is a wealth of private and Federal sector experience among them. I am confident that Jen Easterly, Anne Neuberger, and Chris Inglis have the experience, the talent, and drive to address this issue as well as the many others facing our Nation in the space.

The administration's work has already been seen in CISA's deployment of stopransomware.gov, the U.S. Government's official one-stop location for resources to tackle ransomware more effectively.

But their work is not done. CISA has been plagued by hiring delays, elongated on-boarding processes, a lack of professional human resource specialists, and duplicative and arbitrarily onerous vetting requirements.

It is important that we continue to hold CISA and the Department accountable when it comes to these troubling issues, and I appreciate the Chairwoman working with me on our oversight of the Cyber Talent Management System rollout. I am pleased that CISA Director Jen Easterly has said this will be a top priority during her tenure.

Our concerns are particularly relevant to today's hearing, because no matter how much education we provide to our students, no matter how much interest we cultivate, none of it matters if we can't bring qualified and interested individuals into Government service in a professional and timely manner. Quite simply, we will continue shouting into the wind until we fix these issues.

I look forward to exploring all of these issues with our witnesses today and I hope to hear about concrete proposals for oversight and legislation, not just broad strokes

ideas, which have been the output of similar hearings in the past and have proven ineffective.

I again thank the Chairwoman for holding this timely and important hearing today.

Chairwoman CLARKE. I thank the Ranking Member.

Members of the committee are reminded that the committee will operate according to the guidelines laid out by the Chairman and Ranking Member in their February 3 colloquy regarding remote procedures.

I am looking to see whether our Chairman or Ranking Member have joined us today. They are not present yet, so let me move forward. Statements may be submitted for the record.

[The statement of Chairman Thompson follows:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

JULY 29, 2021

Today's hearing builds on a long-standing priority for the Homeland Security Committee—addressing the shortage of skilled cybersecurity professionals. This problem is not new, but the urgency is greater than ever in light of the increasing number of ransomware attacks and other significant cyber incidents.

Fortunately, the Biden administration has made addressing cybersecurity workforce issues a priority, with Secretary Mayorkas launching a 60-day sprint on strengthening the cyber workforce earlier this year. This decision reflects an understanding that investments in technology are not sufficient on their own—we must also have a well-trained workforce.

In today's digital age, a basic cybersecurity education is essential for everyone, not just cybersecurity professionals. Individuals are vulnerable to cyber criminals, and an employee clicking on a link in a phishing email can expose a company's networks to intruders.

By investing in K–12 cyber education, we improve cyber literacy across the board, while developing a pipeline of young people who can move into more advanced training and join the cybersecurity workforce. Unfortunately, many students currently receive limited cybersecurity education in school today, and the evidence suggests rural and low-income schools with fewer resources are less likely to offer this important training.

The Federal Government can help address this gap by providing resources to schools across the country, offering trainings to teachers, and developing cybersecurity curriculum that can be used nationally. Additionally, by starting education early, we can help address a long-standing concern of mine regarding the cybersecurity workforce—the low number of women and minorities in the field, particularly in senior roles.

I am glad DHS is taking steps to address this through a partnership with the Girl Scouts that will help to educate school-aged girls in cybersecurity and that CYBER.ORG is partnering with HBCUs to help develop a pipeline of Black high school students into cybersecurity programs. These actions demonstrate the important role DHS can and should play in encouraging cyber education. These are important programs, but we'll need a lot more of them to make up for the current gaps. Many cybersecurity jobs are high-paying, and they required a variety of education levels, but many young people may not know about them or may not believe they are attainable.

Federal investment in K–12 cyber education can raise awareness of these career opportunities to more students, increase the diversity of our workforce, and strengthen our National security. Additionally, programs supporting cyber education must continue at higher education institutions and in trainings that can provide cyber skills education to those already in the workforce. DHS's support for the National Centers for Academic Excellence in Cybersecurity and partnerships with other entities like the National labs are important examples of how Government, researchers, and teachers can work collaboratively to address our cyber workforce shortage. DHS must continue to strengthen these partnerships—particularly in collaboration with HBCUs and MSIs—in order to develop the workforce we need to address the varied cyber threats we face today.

I thank Chairwoman Clarke for her leadership in holding this hearing and for prioritizing this critical issue. The excellent witnesses here today have a broad

range of expertise in the field of cybersecurity education and their insights will be valuable as we continue our work in defending the homeland from cyber threats.

Chairwoman CLARKE. I now welcome our panel of witnesses.

First, I welcome Mr. Kevin Nolten, the director of academic outreach for the Cyber Innovation Center at cyber.org. At cyber.org Mr. Nolten helps advance cyber.org's K–12 cyber education program within age-appropriate content that aligns with State standards for education.

Next is Dr. Tony Coulson who serves as the executive director of the Cybersecurity Center at California State University, San Bernardino, and as lead of National Centers of Academic Excellence in Cybersecurity Community.

California State University, San Bernardino is designed at a center of academic excellence in cyber defense education by the National Security Agency and the Department of Homeland Security and it is also a minority-serving institution.

Next is Mr. Ralph Ley, the department manager for Workforce Development and Training Infrastructure within the National and Homeland Security Directorate at Idaho National Labs.

Mr. Ley leads educational programs and research to address cybersecurity issues and work force development needs.

Finally, Max Stier, the president and CEO of the Partnership for Public Service.

In that capacity, he is overseeing the creation and growth of a network connecting more than 1,000 colleges and universities with 80 Federal agencies. He is a thought leader on Federal work force issues and his work is aimed at inspiring a new generation to serve in Government.

Without objection, the witnesses' full statements will be inserted in the record.

I will now ask each witness to summarize his or her statement for 5 minutes, beginning with Mr. Nolten.

STATEMENT OF KEVIN NOLTEN, DIRECTOR OF ACADEMIC OUTREACH, CYBER.ORG, CYBER INNOVATION CENTER

Mr. NOLTEN. Good morning, Chairwoman Clarke, Ranking Member Garbarino, and distinguished Members of the committee. Thank you for the opportunity to testify today.

I am Kevin Nolten, director of cyber.org, an academic initiative of the Cyber Innovation Center, headquartered in Bossier City, Louisiana.

As a nonprofit focused on National security and cybersecurity work force development for the past 4 years, we are supported by Federal grants and contracts, one of which is a Cybersecurity Education Training Assistance Program, as the Chairwoman mentioned, or CETAP, a competitive grant administered by CISA.

One of the greatest threats to our National security is the lack of K–12 cybersecurity education. Recent cyber attacks have demonstrated our vulnerabilities, which can be partially attributed to the growing shortage of cybersecurity professionals.

As a former K–12 administrator, I know the impact K–12 education has on a child's future degree and/or career. A cyber literate population will secure our critical infrastructure. Cyber.org's K–12 cyber education program provides teachers with curriculum and

professional development that align with individual State and local education standard and promotes cybersecurity technical knowledge and degree and career awareness opportunities for students.

Through CETAP we have reached over 23,000 educators in all 50 States. It impacted over 3 million students. We embrace a focus on underserved schools in low socioeconomic regions as 64 percent of all new teachers are from Title 1 schools. We embrace programming specific to ensuring HBCUs have a talent pipeline and that we are focusing on opportunities for students with disabilities.

While we are tremendously proud of the success we have had, however, with nearly 1 million educators and 52 million across the country, our work has just begun.

Chair and Ranking Member, in your home State of New York, 690 educators are accessing the curricula and my team has trained 301 teachers. Further, in all of the subcommittee Members' States combined, over 4,400 educators are accessing the curricula and my team has trained over 3,800 teachers. This is a program that works.

As a recent study shows, high schools using cyber.org's curricula sent four times more students into cyber-related college or university degree programs, such as Cal State San Bernardino. We appreciate that Congress has begun to recognize the importance of cybersecurity education to combat the threats of tomorrow, as CETAP has received bipartisan support.

For example, the Cyberspace Solarium Commission called for additional support for CETAP. As the Chairwoman mentioned, the fiscal year 2021 NDAA formally authorized CETAP within CISA. In fiscal year 2021 CETAP received an increase of funding totalling $6 million.

This year we are requesting that CETAP be funded at $10 million, which would enable further scaling of the program to reach more teachers and ultimately benefiting more students.

As your committee considers the future of cybersecurity education, cyber.org offers the following recommendations: First, we recommend increased and sustained funding for cybersecurity education and work-force development. It is critical that CISA include funding in its annual budget request to expand the reach of CETAP in classrooms across the country. Second, CETAP should be formally recognized as the K–12 feeder program for other Federal cybersecurity work force programs. Third, we recommend special attention be given to the what is next after the different academic milestones, whether K–12, higher education, et cetera, to better connect students directly to cybersecurity jobs.

CISA and cyber.org have made tremendous impact in States across the country, but it is time to scale. Stable continuous funding and legislative support for CETAP will enable the program to reach saturation in all 50 States and grow the talent pipeline. Further investment by Congress to build our National cybersecurity defenses must include K–12 education resources.

Cyber.org appreciates the time to testify and we are willing to serve as a resource for the development of any future cybersecurity education legislation.

Thank you for your time.

[The prepared statement of Mr. Nolten follows:]

PREPARED STATEMENT OF KEVIN NOLTEN

THURSDAY JULY 29, 2021 10 O'CLOCK AM

Good morning, Chair Clarke, Ranking Member Garbarino, and distinguished Members of the House Homeland Security Committee's Subcommittee on Cybersecurity, Infrastructure Protection, & Innovation. Thank you for the opportunity to testify before you today. I am Kevin Nolten, director of CYBER.ORG, the academic initiative of the Cyber Innovation Center, headquartered in Bossier City, LA.

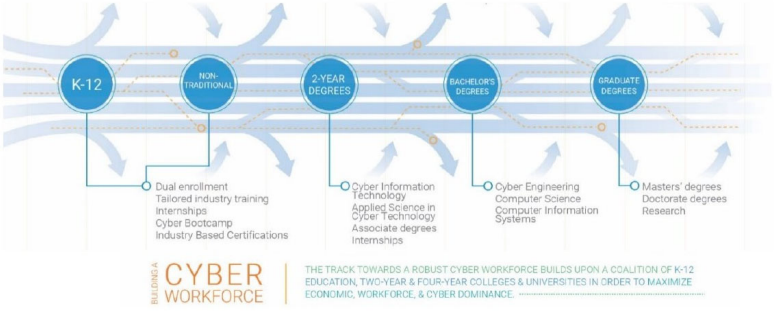
CYBER.ORG is an initiative focused on cybersecurity workforce education and development. CYBER.ORG is appreciative of the support we receive from a grant from the Department of Homeland Security's (DHS) Cybersecurity Infrastructure and Security Agency (CISA) as the lead performer of the Cybersecurity Education Training Assistance Program (CETAP) program.

I commend this subcommittee for seeking to address the long-standing challenges facing cyber workforce development efforts, specifically as they relate to K–12 cybersecurity education and preparing the next generation for the jobs of tomorrow. My testimony will address the role K–12 cybersecurity education plays in creating a foundation of future cyber workers by closing the cybersecurity skills gap and supercharging the future cybersecurity workforce for DHS and industry.

I would first like to provide the subcommittee with a brief overview of my background in education and the origin of CYBER.ORG. Prior to joining CYBER.ORG, I was an educator and school administrator, which provided me with a unique perspective on the education system and the critically important role educators play in providing students with the skills they need to succeed. This ignited my life-long passion for educating students, helping them prepare for their futures and ultimately improving K–12 education Nation-wide. In my role at CYBER.ORG, I direct the organization's programmatic outreach efforts and partnerships with the goal of increasing students' access to K–12 cybersecurity curriculum. At CYBER.ORG, we approach the cybersecurity workforce gap as a National competitiveness issue and believe that increasing cybersecurity literacy will improve U.S. economic and National security. Providing students with an educational foundation and career awareness is imperative to advancing the U.S. cybersecurity workforce.

ABOUT CYBER.ORG

CYBER.ORG is the academic initiative of the Cyber Innovation Center (CIC), an economic development and technology innovation organization focused on growing the regional economy and supporting the National security enterprise through collaboration in mission-critical areas, such as the cybersecurity of our nuclear command, control, and communications systems. The CIC was founded in 2007 with the mission of diversifying the regional economy from primarily oil & gas and agriculture to include 21st Century, knowledge-based jobs in the cyber and information technology (IT) fields. The CIC recognized that to attract cyber and IT companies and jobs, the region would need a ready and able cyber workforce, and building that workforce would require a new approach to education. The success of our model has completely transformed the regional economy in northwest Louisiana: Cyber and IT are now equal to the oil & gas sector in economic impact and jobs. The operational success around cybersecurity the CIC gained at its inception furthered the demand for a comprehensive workforce development program—thus the launch of CYBER.ORG, whose K12 focus represents the entry point onto the Cyber Interstate.



Created in 2011, CYBER.ORG (formerly the National Integrated Cyber Education Research Center or NICERC) identified a specific need in K–12 education for a systematic and integrated solution that would build the foundation for educating the next-generation, cyber-literate workforce. Our goal was to engage K–12 students in STEM, computer science and most importantly, cybersecurity. Since then, we have implemented an integrated curricular experience across multiple academic disciplines through the development of project-driven, hands-on curricula; delivered educator professional development; established K–12 cybersecurity-based pathways; and created National cybersecurity competitions; and.[sic]

CYBER.ORG was initially created using State and local funds but was identified by the Department of Homeland Security in 2011 as an exemplar program and received funding to scale its efforts across the country. As a result of this funding and support, over the last 8 years CYBER.ORG has built a K–12 cyber education program with age-appropriate content that aligns with individual State standards for education. The impact of that work is measured in thousands of teachers and millions of students with access to more content, resources, and training that will fuel the cyber workforce pipeline for the future.

THE CHALLENGE

The United States has been struggling to solve the cyber workforce shortage in this country for too long. The workforce gap that exists today is directly connected to the country's lack of attention to STEM (science, technology, engineering, mathematics) education 15–20 years ago. Very similar to the Space Race, the United States must ensure that our students, the future workforce of our country, are equipped with the knowledge, skills, and abilities to defend against vulnerabilities in cyber space.

CYBER.ORG recognizes this mounting challenge and has built a successful educational model that is critical to ensuring that teachers can teach cybersecurity and students have the skills necessary to meet future workforce needs. The recent, unprecedented cyber attacks like the SolarWinds and Colonial Pipeline clearly demonstrate the adverse effects of our National cybersecurity vulnerabilities, which can in part be attributed to the U.S. workforce shortage. We must increase resources and partnerships with real investments in our future U.S. workforce to ensure we are better equipped to deal with emerging technological threats.

Statistics highlight the urgency of this challenge, as increasingly complex attacks are occurring at a time when there are more than 464,000 unfilled cybersecurity roles in the United States. Filling these positions is essential to protecting both public and private organizations from outside threats, advancing U.S. innovation, and diversifying our country's cybersecurity workforce. The first step toward doing this is educating students on cybersecurity literacy as early as kindergarten.

CYBER.ORG APPROACH—EMPOWER EDUCATORS TO PREPARE THE NEXT GENERATION CYBER WORKFORCE

Advancing the cybersecurity workforce is critical to protecting the country's National security and advancing its cybersecurity posture. K–12 cybersecurity education plays a fundamental role in helping students develop the skills needed to pursue cybersecurity careers in greater numbers. As such, the CETAP Program is crucial to providing the United States with the professional-level expertise needed to solve the cyber challenges of tomorrow, but more can be done to support these efforts. CYBER.ORG has developed a multi-pronged approach to ensuring students Nation-wide have the educational cybersecurity foundation and career awareness needed to advance the National cybersecurity workforce.

QUALITY CURRICULUM AND EFFECTIVE PROFESSIONAL DEVELOPMENT

Through CETAP, CYBER.ORG develops and distributes cyber and cybersecurity curricula to K–12 educators across the country at no cost to the educators. The CYBER.ORG approach supports cybersecurity curriculum development to provide resources for elementary and secondary school teachers that foster foundational cybersecurity awareness, cybersecurity career awareness, and technical cybersecurity skills. The curriculum is mapped to relevant State and National standards and includes resources that make up 20+ full years of curriculum (180+ hours). The curriculum is developed by subject-matter experts in K–12 education, including faculty from higher education institutions across the country and representatives from industry and Government. The CYBER.ORG team, who serve as lead developers, are all experienced educators, many carrying a master's and/or doctorate degree in curriculum and instruction, educational leadership, and educational technology.

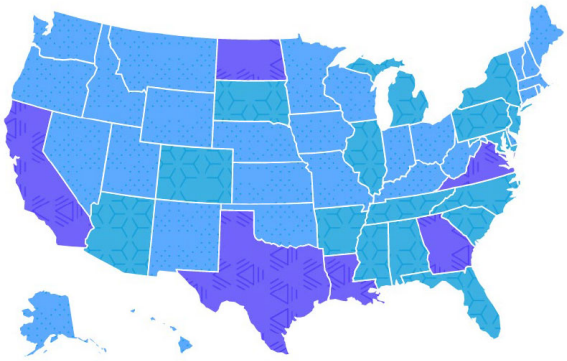
CYBER.ORG currently provides K–12 cybersecurity workforce development assistance to educators in all 50 States, with a cumulative estimated impact of over 3,000,000 students. More than 23,000 teachers are currently enrolled in CYBER.ORG's content platform and over 17,000 teachers have been trained to use CYBER.ORG content for K–12 cybersecurity education.

CYBER.ORG, in August 2021, will publish the country's first set of National K–12 cybersecurity learning standards. Currently, there are only a few models of State-developed cybersecurity standards and no National standards specific to cybersecurity. The goal with the standards is to increased access to cybersecurity education opportunities for students that will prepare them to enter the workforce or to expand their study in college. The standards will take two approaches. The first is ensuring students have a foundational cyber understanding and knowledge to live, work, and play in cyber space safely. The second is ensuring students have the technical skills to pursue industry-based certifications such as CompTIA's IT Fundamentals, A+ and Security+.

NATION-WIDE DEPLOYMENT

Over the past 8 years, CYBER.ORG has been the lead technical institution for CETAP as it has developed and distributed a scalable program for educating the next-generation, cyber-literate workforce through a replicable educational solution for State departments of education, school districts, and individual educators from across the county.

CYBER.ORG has made a significant impact in advancing K–12 cybersecurity education in States across the country thanks to partnerships with Government, educators, and school districts. With both a top-down and bottom-up approach, CYBER.ORG has been able to not only align programs to relevant State standards, help States develop cyber-related standards and pathways, and scale programming throughout the country, but also has been able to provide classroom-specific resources to educators wishing to implement modules on ransomware, or other cybersecurity topics.



https://cyber.org/about-us/our-impact

In addition to partnering with State departments of education, school districts, and classroom teachers, CYBER.ORG also prides itself on engagement with community organizations, non-profits, and industry. For example, in partnership with Palo Alto Networks, CYBER.ORG worked with the Girl Scouts USA to develop 18 cybersecurity badges to introduce more young women to cybersecurity. To date, more than 200,000 cybersecurity badges have been earned by Girl Scouts from across the country.

CYBER.ORG is also working with another global cybersecurity defense contractor to develop a "badging" program to ensure K–12 students have skill sets and industry-based certifications to pursue 2- and 4-year degrees or jump straight into the cybersecurity workforce immediately after high school.

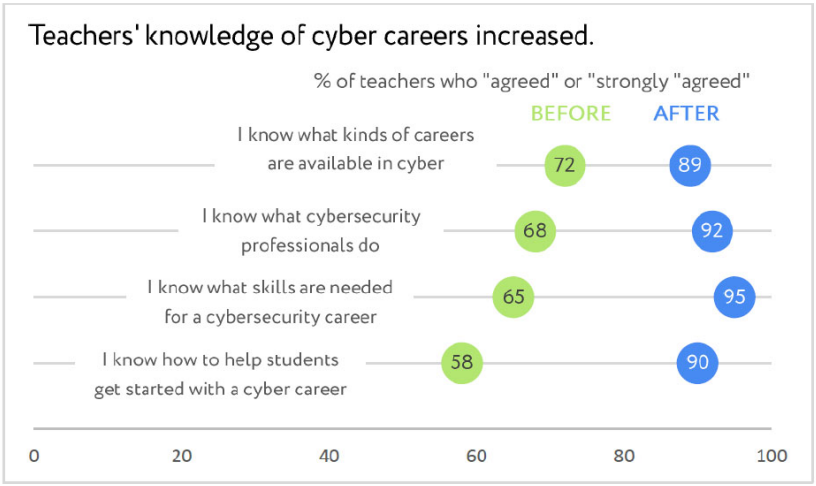
In the National delivery, CYBER.ORG has seen 64 percent of the teachers trained over the past 3 years come from Title 1 schools, that is schools that service students from low socioeconomic communities. Additionally, the efforts around diversifying the cybersecurity workforce have been very deliberate. Recently, CYBER.ORG launched a K–12 Historically Black College and University (HBCU) and Minority Serving Institution (MSI) Feeder Program to further strengthen the talent pipeline and increase the number of minority students pursuing cybersecurity degrees. CYBER.ORG is in the process of developing a K–12 feeder program for Grambling State University (GSU), a HBCU and the first university in Louisiana to create a cybersecurity undergraduate degree. In 2021–2022, CYBER.ORG will replicate this program between minority-serving school districts and HBCUs across the country.

The current reach of the CYBER.ORG curriculum content has impacted student achievement and interest in STEM and cyber career pathways. In a 2021 evaluation conducted by CYBER.ORG, 66 percent of students who completed CYBER.ORG's Cybersecurity course wanted to explore career options in cybersecurity, while 48 percent of students intended to earn at least one cyber-related industry-based certification before graduating from high school.

CONNECTING STUDENTS TO CYBERSECURITY DEGREES AND CAREERS

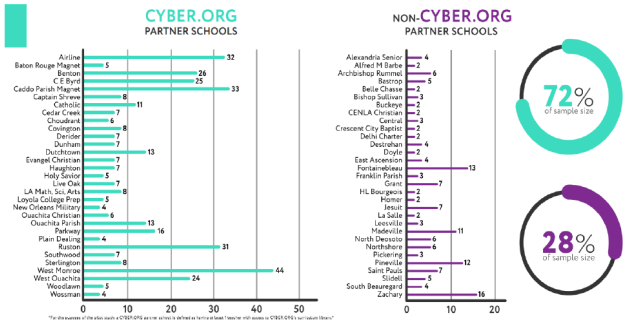
Many studies show that the formative years for a student's career trajectory occur around the middle school level, 6th–8th grade. This period, and the years leading up it, is critical for policy makers, industry, Government, and educators to begin introducing students to 21st-Century options—jobs that many students don't know about, and in some cases jobs that do not yet exist.

CYBER.ORG, as a workforce development organization, ensures teachers have the resources and confidence to prepare students for the next level—whether that is a 2- or 4-year college/university degree, or whether that is direct entry from high school into a cybersecurity career. This confidence is gained through the no-cost professional development offered by the CYBER.ORG team.



In addition to increasing teacher's confidence in introducing their students to cybersecurity careers, CYBER.ORG provides students with Career Profile Cards *(https://cyber.org/career-exploration/cyber-career-profiles)* that introduces them to jobs in cybersecurity. Aligned to the NICE cybersecurity workforce framework, each Career Profile Card teaches students about the job, the skills sets required, the degree (if any) and the certifications (if any) needed for entry into this career.

The multi-faceted approach CYBER.ORG takes yields results. A regional study *(https://cyber.org/sites/default/files/2020-06/Louisiana%20Study.pdf)* found that high schools with teachers enrolled in CYBER.ORG curricula on average sent, in total, four times more students into cyber-related college of university degree programs as those that did not.



INVESTING IN K–12 CYBER EDUCATION

The solution for solving the cybersecurity workforce shortage is developing a capable pipeline of cybersecurity professionals who are entering the workforce at every level of education. CYBER.ORG is enabling K–12 teachers to serve as force multipliers, educating students to build the cybersecurity workforce of the future. The CETAP model and CYBER.ORG have provided a clear blueprint for bolstering the U.S. workforce pipeline for other areas critical to U.S. economic development and global technological competitiveness.

The work being done by CYBER.ORG through the CETAP program also supports the recommendations made by the Cyberspace Solarium Commission. The Commission's report on Growing a Stronger Federal Cybersecurity Workforce [1] called out the importance of the CETAP program in helping recruit the talent needed to support the Federal workforce. The Solarium Commission also identified that the CETAP program has "significant room to grow." To grow, CETAP would need additional funding and resources to:

- Increased access to curricula for educators;
- Development of pathways for immediate job entry, more direct connection of high schools to post-secondary workforce pathways, and engagements with more HBCU institutions;
- Expansion of recruiting and retaining students from military families for future cyber employment;

[1] *https://www.solarium.gov/public-communications/workforce-white-paper*.

- Development of virtual curricula, resources that can be used by schools for student asynchronous learning, particularly in rural and underserved communities; and
- Launch of a virtual cyber laboratory specifically used for K–12 educators, providing an application-based learning environment for real-world cybersecurity lessons.

Congress has recognized the importance of CETAP. With the help of this committee's former Chair Cedric Richmond as well as Senators Rosen and Cassidy, the fiscal year 2021 National Defense Authorization Act (NDAA) formally authorized CETAP and codified the program's mission as a leader in the dissemination of cybersecurity-focused K–12 education resources and training. The fiscal year 2021 authorization was paired with an appropriation of the annual base amount of $4.3 million with an additional discretionary funding of $1.7 million for K–12 education at CISA. With the additional funding, CETAP utilized the additional $1.7 million provided in discretionary support to enable the launch of three K–12 initiatives focusing on Historically Black Colleges and University (HBCU) feeder high schools and students with disabilities.

RECOMMENDATIONS

CYBER.ORG, through CETAP, has made a tremendous impact in States and districts across the country, but it is time to scale. Providing stable, continuous funding and legislative support for CETAP will enable the program to reach its short- and long-term goals of expanding programming in all 50 States so that every student in the United States is cyber literate and has the skills needed to pursue cybersecurity careers in greater numbers and fortify the workforce needed to combat increasingly complex attacks. The following recommendations and actions are important to large-scale impact of CYBER.ORG and CETAP.

- First, we recommend increased and sustained funding for cybersecurity education and workforce development. It is critical that CISA include funding in its annual budget request to sustain and expand the reach of the CETAP program in classrooms across the country. CETAP's cost-effective approach will get proven successful curriculum into the hands of more teachers who will continue to develop a strong, equitable pipeline of cybersecurity talent.
- Second, CETAP should be formally recognized as the K–12 feeder program for other, Federal cybersecurity workforce programs. Connecting students directly to programs such as Centers for Academic Excellence, Scholarship for Service, Federal Apprenticeship Program, and others will ensure these Federal efforts complement one another and provide the best workforce outcomes possible.
- Third, we recommend special attention be given to "what's next" after the different academic milestones (K–12, higher education, reskilling, etc.)—that is, addressing the need for connecting students to cybersecurity jobs. Importantly, connecting students, whether high school, college, university graduates, or nontraditional students to the cybersecurity workforce is a critical step in closing the workforce gap in the country.

CONCLUSION

It has been an honor to appear before this distinguished panel of policy makers. Thank you, Chair Clarke, and Ranking Member Garbarino for your dedication to growing and advancing the cybersecurity workforce.

K–12 cybersecurity education must be viewed as the vehicle in which we can introduce the next generation of cybersecurity professionals to careers in the field. Expanding K–12 cybersecurity education is critical to addressing the cybersecurity workforce shortage. DHS has created a proven, cost-efficient model to train educators in cybersecurity and reach more K–12 students in classrooms across the country with cybersecurity curriculum. The CETAP program requires additional investment to close the cybersecurity workforce gap and grow the cybersecurity skills pipeline.

CYBER.ORG envisions a future where every student is cyber literate and has the option to pursue cybersecurity careers. We look forward to working with the committee and serving as a resource as it develops policies to advance K–12 cybersecurity. We also remain committed to working with committee Members in their States and districts to advance the CETAP program and expand access to K–12 cybersecurity education.

CYBER.ORG appreciates the opportunity to join in this worthy discussion and is willing to serve as a resource in the development of any cybersecurity education legislation going forward. We are thrilled to participate in today's hearing and look for-

ward to a long partnership where we can continue working to tackle this important issue.

Thank you, and I'll be happy to answer any of your questions.

Chairwoman CLARKE. Thank you, Mr. Nolten, for your testimony.

I now recognize Dr. Coulson to summarize his statement for 5 minutes.

STATEMENT OF TONY COULSON, PH.D., PROFESSOR AND EXECUTIVE DIRECTOR, CYBERSECURITY CENTER LEAD, NATIONAL CENTERS OF ACADEMIC EXCELLENCE IN CYBERSECURITY COMMUNITY

Mr. COULSON. Chairwoman Clarke, Ranking Member Garbarino, Members of the Cybersecurity Infrastructure Protection Innovation Subcommittee, thanks for having me.

I am Tony Coulson from Cal State San Bernardino. We are a Hispanic-serving institution location in southern California. We have, under the leadership of Dr. Tomás Morales, expanded to over 20,000 students and are ranked 7th nationally for social mobility. But one thing we are known for is innovation.

Now, you might ask yourself what does a regional university in California have to do with cybersecurity, and it is actually very simple. As has already been mentioned, we have a cybersecurity work force shortage. We know we have a crisis. I just looked up the number earlier before we came on, we have over 500,000-person shortage—500,000. Let that number sink in. This came from cyberseek.org. That is an absurd number. If this was doctors and nurses there would be a National outcry.

Well, the good news is Cal State San Bernardino is committed to solve this work force problem. Recently our university established and began to lead the National Centers of Academic Excellence Cybersecurity Community. This community involves 5 Federal partners, the NSA, National Security Agency, who runs the program, DHS and CISA, NIST, and the NICE Initiative, as well as the FBI and the Department of Energy. Those Government partners are now coupled with the CAE community, the Centers of Academic Excellence community that we lead that has 335 colleges and universities working together to collaborate and solve the work-force shortage.

Now, working with these partners, and also working with all of these universities, we have a lot of creativity and we have a lot of collaboration, but we also have an interesting vantage point where we see gaps and we see silos and we see duplication. We are trying to develop solutions. As cyber.org and Kevin, good friends, just said, look, we know that K–12 is a huge opportunity. There is a lot of activity in this space and there is a lot of investment through a lot of agencies. But there are still gaps. There is a lot of work to be done here, such as we need to increase diversity, but also in rural and home school networks.

So the Centers of Academic Excellence community just released a program focusing on rural and home school. We just helped get AP cyber onto the National curriculum. We are putting together extracurriculars, such as camps and cyber competitions. Matter of fact, the gen cyber program at Cal State San Bernardino that we originally partnered with cyber.org, the genesis of that camp at Cal

State San Bernardino that has now affected thousand of kids, led to a national Girl Scout badge.

But it is more than K–12. The United States is facing a deficit in cyber research. We need to home-grow research skill. So Cal State San Bernardino and its partners in the community just launched the Information Security Research Education Program, a unique program where we take technical directors from the National Labs and the National Security Agency and others and work with student teams around the country in a variety of different institutions to solve real-world technical problems.

Access is also a problem, access to technology, but also are we getting the return on investment, are we producing work-force ready students? Well, Cal State San Bernardino created the NICE Challenge Project, a National cyber range in use by 500 colleges and universities that provides technology and does work-force readiness assessment.

These are a lot of programs and there is a lot of things. I will tell you this, the Centers of Academic Excellence Community, those 335 schools, colleges, and universities that are working together today are producing over 100,000 diverse quality students, reskilling people, working with veterans, working in our communities. This is all based on one-time funding and most of it has come from the National Security Agency. What I would like to see is I would like to see the Department of Homeland Security move forward and support with sustainable funding such an important initiative.

Thank you so much for your time today.

[The prepared statement of Dr. Coulson follows:]

PREPARED STATEMENT OF TONY COULSON

JULY 29, 2021

Chairwoman Clarke, Ranking Member Garbarino, and Members of the Cybersecurity, Infrastructure Protection, & Innovation Subcommittee, I want to thank you for providing me with the opportunity to testify today. My name is Professor Tony Coulson and I serve as the executive director of the Cybersecurity Center at California State University, San Bernardino (CSUSB).

CSUSB is one of 23 campuses that make up the great California State University system—the largest 4-year public university system in the world. Under the leadership of President Tomás Morales, CSUSB is a Nationally-recognized university, serving more than 20,000 students, most of whom come from the Riverside and San Bernardino counties, an area in inland Southern California known as the Inland Empire. As a Hispanic-Serving Institution (HSI), we are recognized for our transformative influence in our community. More than 80 percent of CSUSB's students are the first in their families to earn 4-year college degrees, and two-thirds of our students come from economically-disadvantaged circumstances. We are proud that CSUSB, with campuses San Bernardino and Palm Desert, is ranked No. 7 among top colleges and universities educating economically disadvantaged students and graduating them into well-paying jobs. CSUSB is recognized globally for our Jack H. Brown College of Business and Public Administration and Nationally for our leadership in developing the country's cybersecurity workforce.

I am here today to specifically talk about ways how to bridge the Nation's cybersecurity workforce gap, how CSUSB's Cybersecurity Center is currently leading Nation-wide initiatives in this effort, and how existing U.S. Government programs are working with universities like mine to achieve this goal. More than 12 years ago, CSUSB created its Cybersecurity Center ("Center"), focused on one mission—creating a cybersecurity talent pool and a corresponding job base within the Inland Empire region of California. This has always been a clear need as the Inland Empire has been an economically depressed region for the last two decades, experiencing economic challenges like so many of our communities across the Nation, but

with one of the lowest degree attainment rates in the State of California combined with low high school graduation rates.

To address these issues, CSUSB created a Cybersecurity Center with four undergraduate programs in a variety of disciplines including criminal justice, business and public administration, computer science, and information science. This led us to develop five master's degree programs along the same disciplines (business, computer science, information systems, and public administration) but with one broader goal, to integrate the NSA Centers of Academic Excellence in Cybersecurity with the Intelligence Community CAE program—creating a critical new program to produce intelligence analysts with cyber skills. This new master's program in National Cybersecurity Studies became a model curriculum adopted by universities around the United States. From 12 years ago with 10 students, CSUSB now has over 600 students enrolled in these degree programs. While CSUSB has always been innovative in its approach, providing an environment that built curriculum based on Government and industry workforce needs, it was the students that provided the energy and truly showed their capabilities.

CSUSB is on the front line training the next generation of cyber warriors. We are proud to say that CSUSB's student outcomes are so strong that one program director at the U.S. Department of Homeland Security (DHS) once said that CSUSB students "are everywhere" and have commended the skill sets that CSUSB students have when they graduate.

The Nation has had a dearth of well-trained cybersecurity workers for many years; however, the problem is greatly exacerbated by the integration of technology into every sector of our economy, leading to an inevitable growth of cybersecurity attacks. These attacks have illustrated the need to expeditiously fill the estimated 500,000-person deficit in the Nation's cybersecurity workforce. As part of my testimony today, I want to stress the importance of partnerships across academia, with the Government, as well as with industry. The 2020 Cyberspace Solarium Commission report states that " . . . sometimes success in building a robust Federal workforce depends on elements outside of the Federal Government. In those cases, the U.S. Government can and should play a supporting role by providing its partners in workforce development the tools needed to accelerate the increase in cyber personnel."

A 2021 report on "The Hewlett Foundation's Cyber Talent Pipeline: An Evolution Based on Equitable Evaluation Framework Principles" states "We identified 5 Minority-Serving Institutions to be in our evaluation sample; each has committed cyber faculty, existing innovative partnerships and the opportunity to further develop interdisciplinary education programs . . . Cal State San Bernardino leads a National collaboration of more than 300 universities and colleges dedicated to cyber and piloting innovations, many of which are community colleges." The report also states that "the assumption that elite universities are best placed to enable multidisciplinary cyber education is not borne out by our evidence."

Just as President John F. Kennedy called for a greater goal for the United States to land a man on the moon, so must we as a Nation think about the global cyber race. In his speech before a Joint Session to Congress on May 25, 1961, the needs that President Kennedy highlighted still resonate today: "I believe we possess all the resources and talents necessary. But the facts of the matter are that we have never made the National decisions or marshaled the National resources required for such leadership. We have never specified long-range goals on an urgent time schedule, or managed our resources and our time so as to insure their fulfillment."

I am happy to be here today to discuss this important challenge, describe what CSUSB is doing to help address the problem, discuss key Federal partnerships we have and the outcomes they are producing, and to share best practices for how we can address this problem head-on together.

I. CSUSB AND THE NATIONAL CENTERS OF ACADEMIC EXCELLENCE IN CYBERSECURITY (NCAE–C)

The National Centers of Academic Excellence in Cybersecurity (NCAE–C) program was created in 1999, beginning with just 7 schools, and through its successful partnerships, the program has grown to 335 schools across 48 States.[1] The NCAE–C program is the Nation's premier cyber workforce development initiative that leverages the unique capabilities of the National Security Agency (NSA) and the member schools to meet the Nation's needs for a specialized education program and unique curricula. NCAE–C is the first, and only of its kind, to have clearly defined

[1] See Attachment A: List of schools in the NCAE–C program.

academic standards, curricula, and designations for cyber education, holding the member colleges and universities to rigorous educational standards.

CSUSB's Cybersecurity Center is part of the NCAE–C system and leads the Centers of Academic Excellence in Cybersecurity Community. Six years ago, there were 100 institutions in the program, now there are 335 NSA–Designated Centers of Academic Excellence in Cybersecurity, educating approximately 100,000 students in cyber-related disciplines.

The CAE Community in Cybersecurity program allows for innovation with our Government partners at NSA, the Program Office, as well as DHS, the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the National Initiative for Cybersecurity Education (NICE), and the National Science Foundation (NSF).

These partnerships are important as each agency plays a unique role in the CAE program. To help increase a talent pipeline for students into the Federal Government, DHS serves as a strategic partner in promoting cybersecurity education and workforce development, as well as strengthening partnerships between institutions and Federal, State, local, and Tribal governments.

II. CSUSB AND CYBER CORPS®: SCHOLARSHIP FOR SERVICE

A strong example of the benefit of partnerships is NSF's CyberCorps®: Scholarship for Service program. This program has sponsored thousands of cybersecurity students leading them into Government cyber careers. This unique partnership with DHS, NSF, OMB, and the NSA CAE Program has produced thousands of quality cybersecurity graduates as well as building capacity for stronger cyber research and programs at colleges and universities. DHS and NSF further expanded the CyberCorps® program by creating the Community College Cybersecurity Pilot scholarship program focused on veterans and persons with existing bachelor's degrees.

III. CSUSB FOCUS ON K–12 PROGRAMS

CSUSB has a long-standing commitment to focusing not just on college-age students, but also on going deeper into the educational pipeline to start teaching cybersecurity skills to younger students. A great example of this is CSUSB's involvement in the GenCyber program—a partnership between the NSF and the NSA. The GenCyber program provides K–12 students the opportunity to go to "cybersecurity summer camp" for free and for teachers to participate in training camps to provide cyber literacy in the classroom. CSUSB's early work in this program involved partnerships with the Girl Scouts of San Gorgonio Council as well as Title I middle schools, to reach underserved communities and promote diversity in cybersecurity talent. This successful series of camps serving over 1,200 girls eventually led to a National Girl Scout badge in cybersecurity.

Through recent grant programs, the greater CAE Community schools are working together to create K–12 learning pathways to provide cyber literacy programs and prepare students for cyber careers. Cybersecurity teachers in schools around the country are learning new skills to teach cybersecurity and in doing so utilizing freely available CAE materials and those developed by our partners. The new Regions Investing in the Next Generation (RING) program from Illinois' Moraine Valley Community College and Alabama's University of Alabama Huntsville focuses on teaching cybersecurity skills in rural areas and home schools and provide resources for diverse communities including the economically disadvantaged, the deaf and hard of hearing, and the neurodiverse. Additionally, New York's Mohawk Valley Community College and Florida's University of West Florida have just launched the national Enigma cybersecurity competition. This National competition starts with 165 12-person teams (1,980 high school students) to attack and defend in unique cyber scenarios as well as interact with potential employers. The CAE Community now has year-round extracurricular and in-school activities focused on cyber in K–12.

IV. CREATING CUTTING-EDGE PROGRAMS:—INSURE (INFORMATION SECURITY RESEARCH EDUCATION)

Federal grants have also funded future-oriented programs, meaning that CAE Community schools and Government partners are not just focusing on the cybersecurity skills of today but also are looking at the cybersecurity skills that are needed 5 years from now and beyond.

Recognizing a shortage of domestic research talent, CSUSB, working with the NSF, NSA, and CAE Community partners, has advanced a cutting-edge research program. Housed at CSUSB, this program, called the Information Security Research Education (INSuRE) program, works with technical directors from industry, the

U.S. Department of Energy (DOE), National labs, DHS, and the NSA, to partner with student teams around the country on real cybersecurity problems. The CAE Community is listening to industry and Government needs, adapting its curriculum, and focusing on research in artificial intelligence (AI), autonomous vehicles (AV), advanced networks, and critical infrastructure protection.

V. CSUSB PARTNERING WITH COMMUNITY COLLEGES AND THE NATIONAL SCIENCE FOUNDATION ADVANCED TECHNOLOGY EDUCATION (ATE)

CSUSB's collaboration and partnership mission is further evident with the cooperation of the NSA and the NSF's Advanced Technology Education (ATE) program. The National Cybersecurity Training and Education Center, based at Whatcom Community College in Washington State, focuses on opportunities and the development of cybersecurity workforce capabilities at community colleges Nationwide, and working with the CAE Community, established a National Cybersecurity Virtual Career Fair to match students from CAE colleges and universities with employers across the Nation. In 2020, this career fair saw more than 1,400 well-qualified CAE students and 38 employers participate. This year, the CAE Community is seeking to double that number. Future collaborations include National apprenticeship initiatives partnering with CAE-designated schools.

VI. CSUSB PARTNERSHIP WITH THE NICE CHALLENGE PROJECT

Another strong example of how CSUSB's successful cybersecurity collaboration is the CAE Community's National cyber range, the NICE Challenge Project. The program is funded through grants from NSF, DHS, NSA, and the NICE program with a mission to create a range where cybersecurity participants can test their cyber workforce readiness, measured against the NIST Cybersecurity Workforce Framework (800–181) and NSA Knowledge Unit Standards. This system, free for use in higher education, currently serves thousands of students at 500 schools across the Nation. This program is exploring an expansion for helping veterans, and high schools, and working with CISA on Federal workforce training. With further funding from DHS, CISA, and NSA, this cyber range could be easily scaled to serve the Nation's high schools, providing progress toward workforce readiness. Working with CISA, CSUSB also sees opportunities for using the NICE Challenge as a means to train, develop, and validate the Federal workforce.

VII. LOOKING AHEAD

The Nation is grappling with a critical problem to address the cyber workforce challenge. Colleges and universities across the country are doing tremendous work to address the problem and CSUSB is doing its part each day to help bridge the workforce gap. As Congress grapples with solutions to these challenges, it must avoid creating new programs in the Federal Government, but rather provide steady-state funding to ones that are in existence and have a long history of success. The CAE Community has existed for 22 years and has amazing return on investment using Federal funds. Other programs such as those I have described at NSF and NIST, working with the DHS and other agencies, are successful programs making great strides to address the problem.

What makes the CAE Community program unique is its willingness to collaborate with a wide range of entities, from both industry and Government, as a critical resource. DHS has a unique vantage point based on its mission to safeguard the Nation's homeland, and DHS should promote sustained funding and leverage the capabilities of the CAE Community in its efforts to address cybersecurity workforce challenges.

The colleges and universities that make up the CAE in Cybersecurity Community have boundless energy, but what is needed from Congress is a concerted focus and dedicated funding for all of these programs along with the need to avoid creating overlapping and duplicative programs across all other agencies. The model created in the CAE community, working with DHS, FBI, NSF, and NIST have a long history of success. The program is also created and run by those who understand cybersecurity and the educational needs of our community. We need to sustain and encourage the non-profit, collaborative approaches that work and dedicated funding is critical to helping to achieve these goals.

We also need to ensure the workforce of the future is diverse in nature as well. The CAE Community schools are engaged in many initiatives building out diverse workforce, including wounded warriors, neurodiverse, women, and minority-serving institutions. The recently-launched Cyber Education Diversity Initiative (CEDI) is housed at Fordham University in New York State. This program is focused on building the capacity of minority-serving institutions (MSIs) to become CAE-designated

as well as inviting students from MSIs to join competitions, hosting workshops for faculty, and allowing for students to transfer from MSIs to colleges with a cybersecurity degree program.

NATO Secretary General Jens Stoltenberg, speaking at the Cyber Defence Pledge Conference in London in 2019, stated: "It takes just a 'click' to send a cyber virus spreading across the globe. But it takes a global effort to stop it from inflicting chaos." He went on to say "But cyber goes beyond technology. The people behind the technology are just as important. We need to build a strong and diverse workforce of future cyber defenders."

The efforts by CSUSB and the Centers of Academic Excellence in Cybersecurity Community have generated undeniable results but tackling a 500,000-person workforce shortage is a problem that will require "all hands-on deck." Where there are programs that already exist with long-standing demonstrable results, Congress should support those with dedicated funding. Thank you for your time and I look forward to any questions.

ATTACHMENT.—NSA DESIGNATED CENTERS OF ACADEMIC EXCELLENCE IN CYBER INSTITUTIONS

Athens State University—AL
Auburn University—AL
Calhoun Community College—AL
Jacksonville State University—AL
Snead State Community College—AL
The University of Alabama—AL
The University of Alabama at Birmingham—AL
The University of Alabama in Huntsville—AL
Tuskegee University—AL
University of South Alabama—AL
University of Arkansas—AR
University of Arkansas at Little Rock—AR
Arizona State University—AZ
Embry-Riddle Aeronautical University, Prescott Campus—AZ
Estrella Mountain Community College—AZ
Glendale Community College—AZ
Grand Canyon University—AZ
The University of Arizona—AZ
University of Advancing Technology—AZ
California State Polytechnic University, Pomona—CA
California State University, San Marcos—CA
California State University, Sacramento—CA
California State University, San Bernardino—CA
City College of San Francisco—CA
Coastline Community College—CA
Cypress College—CA
Long Beach City College—CA
National University—CA
Naval Postgraduate School—CA
Ohlone College—CA
Sierra College—CA
University of California, Davis—CA
University of California, Irvine—CA
Arapahoe Community College—CO
Colorado School of Mines—CO
Colorado State University—Pueblo—CO
Colorado Technical University—CO
Pikes Peak Community College—CO
Pueblo Community College—CO
Red Rocks Community College—CO
Regis University—CO
United States Air Force Academy—CO
University of Colorado, Colorado Springs—CO
University of Denver—CO
University of Connecticut—CT
University of New Haven—CT
Georgetown University—DC
The George Washington University—DC
University of Delaware—DE

Wilmington University—DE
Daytona State College—FL
Embry-Riddle Aeronautical University—Daytona Beach Campus—FL
Florida A&M University—FL
Florida Atlantic University—FL
Florida Institute of Technology—FL
Florida International University—FL
Florida State College at Jacksonville—FL
Florida State University—FL
Indian River State College—FL
Nova Southeastern University—FL
Saint Leo University—FL
St. Petersburg College—FL
University of Central Florida—FL
University of Florida—FL
University of North Florida—FL
University of South Florida—FL
University of West Florida—FL
Valencia College—FL
Augusta Technical College—GA
Augusta University—GA
Columbus State University—GA
Georgia Institute of Technology—GA
Georgia Southern University—Armstrong Campus—GA
Georgia State University—GA
Kennesaw State University—GA
Middle Georgia State University—GA
Middle Georgia State University—MSIT—GA
University of Georgia—GA
University of North Georgia—GA
Honolulu Community College—HI
Leeward Community College—HI
University of Hawaii—West Oahu—HI
University of Hawaii at Manoa—HI
University of Hawaii Maui College—HI
Iowa State University—IA
Idaho State University—ID
North Idaho College—ID
University of Idaho—ID
College of DuPage—IL
DePaul University—IL
Illinois Institute of Technology—IL
Illinois State University—IL
John A Logan College—IL
Lewis University—IL
Lincoln Land Community College—IL
Loyola University Chicago—IL
Moraine Valley Community College—IL
Rock Valley College—IL
Roosevelt University—IL
University of Illinois at Springfield—IL
University of Illinois, Urbana—Champaign—IL
Indiana University—IN
Ivy Tech Community College—IN
Purdue University—IN
Purdue University Northwest—IN
Butler Community College—KS
Fort Hays State University—KS
Johnson County Community College—KS
Kansas State University—KS
University of Kansas—KS
Wichita State University—KS
Bluegrass Community and Technical College—KY
Murray State University—KY
Northern Kentucky University—KY
Owensboro Community and Technical College—KY
University of Louisville—Graduate Certificate of Cybersecurity—KY
University of Louisville, Kentucky—KY

University of the Cumberlands—KY
Bossier Parish Community College—LA
Louisiana Tech University—LA
University of New Orleans—LA
Boston University—MA
Northeastern University—MA
University of Massachusetts Lowell—MA
Worcester Polytechnic Institute—MA
Anne Arundel Community College—MD
Bowie State University—MD
Capitol Technology University—MD
Cecil College—MD
College of Southern Maryland—MD
Hagerstown Community College—MD
Harford Community College—MD
Howard Community College—MD
Morgan State University—MD
Prince George's Community College—MD
The Community College of Baltimore County—MD
The Johns Hopkins University—MD
Towson University—MD
United States Naval Academy—MD
University of Maryland—MD
University of Maryland Global Campus—MD
University of Maryland, Baltimore County—MD
Southern Maine Community College—ME
University of Maine at Augusta—ME
Baker College—MI
Davenport University—MI
Delta College—MI
Eastern Michigan University—MI
Ferris State University—MI
Grand Rapids Community College—MI
Henry Ford College—MI
Lansing Community College—MI
Macomb Community College—MI
Oakland University—MI
University of Detroit, Mercy—MI
Walsh College—MI
Washtenaw Community College—MI
Capella University—MN
Century College—MN
Lake Superior College—MN
Metropolitan State University—MN
St. Cloud State University—MN
Walden University—MN
Metropolitan Community College—Kansas City—MO
Missouri University of Science and Technology—MO
Southeast Missouri State University—MO
St. Louis Community College—MO
University of Missouri—Columbia—MO
University of Missouri—St. Louis—MO
Webster University—MO
Mississippi State University—MS
Great Falls College Montana State University—MT
Missoula College—MT
Alamance Community College—NC
East Carolina University—NC
Fayetteville Technical Community College—NC
Forsyth Technical Community College—NC
Montreat College—NC
North Carolina A&T State University—NC
North Carolina State University—NC
Pitt Community College—NC
Sampson Community College—NC
University of North Carolina, Charlotte—NC
University of North Carolina, Wilmington—NC
Wake Technical Community College—NC

Bismarck State College—ND
North Dakota State University—ND
Bellevue University—NE
Metropolitan Community College—NE
Northeast Community College—NE
University of Nebraska, Omaha—NE
Dartmouth College—NH
University of New Hampshire—NH
Brookdale Community Collge—NJ
County College of Morris—NJ
Fairleigh Dickinson University—NJ
New Jersey City University—NJ
New Jersey Institute of Technology—NJ
Rutgers, The State University of New Jersey—NJ
Stevens Institute of Technology—NJ
Central New Mexico Community College—NM
Eastern New Mexico University—Ruidoso Branch Community College—NM
New Mexico Tech—NM
University of New Mexico—NM
College of Southern Nevada—NV
University of Nevada, Las Vegas—NV
University of Nevada, Reno—NV
Binghamton University (SUNY at Binghamton)—NY
Excelsior College—NY
Fordham University—NY
Mercy College—NY
Mohawk Valley Community College—NY
New York Institute of Technology—NY
New York University—NY
Pace University—NY
Rochester Institute of Technology—NY
Rockland Community College—NY
Syracuse University—NY
University at Albany, the State University of New York—NY
University at Buffalo, the State University of New York—NY
Utica College—NY
Utica College—MS Cybersecurity—NY
Westchester Community College—NY
Air Force Institute of Technology—OH
Cedarville University—OH
Clark State Community College—OH
Columbus State Community College—OH
Franklin University—OH
Sinclair Community College—OH
Terra State Community College—OH
The Ohio State University—OH
University of Cincinnati—OH
Wright State University—OH
Oklahoma City Community College—OK
Oklahoma State University—OK
Rose State College—OK
University of Tulsa—OK
Chemeketa Community College—OR
Mt. Hood Community College—OR
Portland Community College—OR
Portland State University—OR
Bloomsburg University of Pennsylvania—PA
Carnegie Mellon University—PA
Drexel University—PA
East Stroudsburg University—PA
Indiana University of Pennsylvania—PA
Lehigh Carbon Community College—PA
Pennsylvania Highlands Community College—PA
Pennsylvania State University—PA
Pittsburgh Technical College—PA
Robert Morris University—PA
Saint Vincent College—PA
University of Pittsburgh—PA

Valley Forge Military College—PA
West Chester University of Pennsylvania—PA
Polytechnic University of Puerto Rico—PR
Community College of Rhode Island—RI
New England Institute of Technology—RI
University of Rhode Island—RI
Clemson University—SC
South Carolina State University—SC
The Citadel—SC
Trident Technical College—SC
University of South Carolina—SC
Dakota State University—SD
Jackson State Community College—TN
LeMoyne—Owen College—TN
Roane State Community College—TN
Tennessee Tech University—TN
The University of Tennessee at Chattanooga—TN
University of Memphis—TN
El Paso Community College—TX
Hill College—TX
Houston Community College—TX
Laredo College—TX
McLennan Community College—TX
Our Lady of the Lake University—TX
Sam Houston State University—TX
San Antonio College—TX
South Texas College—TX
Southern Methodist University—TX
St. Philip's College—TX
Texas A&M University—TX
Texas A&M University—Corpus Christi—TX
Texas A&M University—San Antonio—TX
Texas State Technical College in Harlingen—TX
The University of Texas at Austin—TX
The University of Texas at San Antonio—TX
University of Dallas—TX
University of Houston—TX
University of North Texas—TX
University of Texas at Dallas—TX
University of Texas at El Paso—TX
Brigham Young University—UT
Southern Utah University—UT
Danville Community College—VA
ECPI University—VA
George Mason University—VA
Germanna Community College—VA
Hampton University—VA
James Madison University—VA
Liberty University—VA
Lord Fairfax Community College—VA
Marymount University—VA
Mountain Empire Community College—VA
Norfolk State University—VA
Northern Virginia Community College—VA
Old Dominion University—VA
Radford University—VA
Regent University—VA
Southwest Virginia Community College—VA
Thomas Nelson Community College—VA
Tidewater Community College—VA
University of Virginia—VA
Virginia Commonwealth University—VA
Virginia Polytechnic Institute and State University—VA
Virginia Western Community College—VA
Champlain College—UT
Norwich University—UT
City University of Seattle—WA
Columbia Basin College—WA

Edmonds Community College—WA
Green River College—WA
Highline College—WA
Spokane Falls Community College—WA
University of Washington—WA
Whatcom Community College—WA
Madison College—WI
Marquette University—WI
University of Wisconsin—Stout—WI
Waukesha County Technical College—WI
American Public University System—WV
Blue Ridge Community and Technical College—WV
West Virginia University—WV

Chairwoman CLARKE. Thank you, Dr. Coulson.

I now recognize Mr. Ley to summarize his statement for 5 minutes.

STATEMENT OF RALPH F. LEY, DEPARTMENT MANAGER, WORKFORCE DEVELOPMENT AND TRAINING INFRASTRUCTURE ASSURANCE & ANALYSIS DIVISION, NATIONAL & HOMELAND SECURITY, IDAHO NATIONAL LABORATORY

Mr. LEY. Thank you, Chairwoman Clarke, Ranking Member Garbarino, and Members of the committee. It is an honor and a privilege to be with you today.

My name is Ralph Ley. I am the department manager for Workforce Development and Training within the National and Homeland Security Directorate at Idaho National Laboratory. I am grateful for the opportunity to testify on the issues regarding the Nation's cyber talent pipeline and ways to ensure our work force is ready to meet future threats.

As you probably all know, INL's long history with nuclear energy from its inception to the latest and recent work with small modular nuclear reactors, other energy sources, our one-of-a-kind wireless ranges and the wireless networks that are continuing to expand across the United States, various infrastructures and their test beds helping industry. It is easy to understand why we have a deep understanding for industrial control systems, control systems in general and how to protect them. In fact, the Cyberspace Solarium Commission called out INL as the Nation's center of excellence for industrial control system cybersecurity issues. Well-founded.

Our department takes great pride in having the opportunity and responsibility to lead, influence, and execute a broad portfolio of educational programs and research that address IT and OT cybersecurity issues and work force development needs. Although INL supports and has its own numerous K–12 cybersecurity initiatives and the great work, as you can see already some of the witnesses have testified, fantastic work, my primary focus today is to talk about issues relating to the post-secondary education institutes and existing work force already in business and Government agencies. That is an area that needs to be addressed and very quickly.

For over 15 years DOE and DHS have asked us to provide ICS cybersecurity training courses to private-sector businesses, utilities, and Government agencies. The desired result was for participants to become aware of the difference between IT and OT networks and systems, how they interact with each other on the job, the IT and OT experts on businesses, and to develop projects within academia

and industry to better understand the issues surrounding the cyber education of the Nation's work force—what are the impediments and influences in driving the cyber health, if you will, of organizations. One of our latest projects and documents you may have seen is in collaboration with Idaho State University, La Trobe University, titled "Building an Industrial Cybersecurity Workforce: A Manager's Guide". This is just a first attempt and first product that we have developed to address the job roles required by ICS professionals and how an organization may establish a capable work force. NIST has recognized the value of our efforts and has asked us to join them in building out their NICE framework that focuses on IT cybersecurity and move it into and incorporate segments and areas and issues surrounding the OT or industrial control systems as well.

To further flush out issues that need to be addressed: We have also established our own industrial cybersecurity community to practice. One hundred fifty participants from the universities, industries, organizations from around the Nation and internationally to look at the issues.

The recurring issues that are most prominent and that need to be addressed are, as I have listed in the testimony, standardizing curriculum for cyber degrees, establishing a shared repository for cybersecurity curriculum so that all institutes, large and small, can have access to it. But our main focus here is to—and we recommend the focus of energy to help industry organizations understand what their actual cyber job roles are and the educational needs. We find many don't even understand what their organizations need in cyber job roles and leading to the education of those individuals, and also how to hire the right individuals.

There are many other issues out there that need to be addressed, but those are the two areas that we need to look at.

I appreciate the opportunity to testify and I want to thank you again for your attention to this very important issue of our Nation and I look forward to your questions on cybersecurity and the work force and increasing the flow of the cyber talent pipeline.

[The prepared statement of Mr. Ley follows:]

PREPARED STATEMENT OF RALPH F. LEY

JULY 29, 2021

Chairwoman Clarke, Ranking Member Garbarino, and Members of the committee, it is an honor and privilege to be with you today. My name is Ralph Ley, and I am the department manager for workforce development and training within the national and homeland security directorate at Idaho National Laboratory (INL). I'm grateful for the opportunity to testify on issues regarding the Nation's cyber talent pipeline and ways to ensure our workforce is ready to meet future threats.

I want to thank this subcommittee for addressing what we believe is a foundational workforce development and education issue facing this Nation from the standpoint of a continuously changing cyber threat landscape requiring professionals who have career-long access to updated curriculum containing new tactics, techniques, and procedures to sufficiently protect their networks and systems.

Our conversation today is an important step forward for establishing a unified team with a focused approach toward implementing solutions to cyber workforce issues and progress—our security will benefit from this unified effort, it is greatly needed and appreciated.

INL's Nationally-recognized expertise in industrial control systems (ICS) or operational technology (OT) cybersecurity stems from its long history and primary mission to conduct research, development, and demonstration of solutions that assure

the advancement of nuclear energy, clean energy, and critical infrastructure protection technologies. From the beginning related infrastructure were full of control systems to ensure their safe and efficient operations. My department takes great pride in having the opportunities and responsibilities to lead, influence, and execute a broad portfolio of educational programs and research which address cybersecurity issues and workforce development needs.

For over a decade Department of Energy (DOE) and Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) sponsored ICS cybersecurity training courses have been conducted at INL in immersive classroom and hands-on learning environments. The target audience has been primarily private-sector businesses and utilities who need their staff to understand the differences between protecting IT and OT networks and systems. Simply put, IT cybersecurity is based on keeping a business's information readily available, accurate, and dependable, whereas OT cybersecurity lives in a cyber-physical world manipulating businesses assets which can impact production and throughput/output of materials. These sponsored courses offered by INL are designed to bridge the knowledge gap by bringing together people who operate either their company's IT systems or OT systems and force them to work together in realistic work settings. The results of these courses accompanied by the significant increase in recent threats to OT systems has contributed heavily to industry's awareness, or better described—awakening—to the need for improved OT cybersecurity practices accompanied by established standards for workforce development and training.

Processes and procedures for securing IT systems are well-documented in a wide variety of general overarching best practices and some industry-specific standards. The same guidance has been late coming for securing OT systems, however this guidance is now much more readily available than even just a few years ago. Along with established cybersecurity procedures or standards has been guidance on what education and training is required by cyber professionals to implement these new measures.

The National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) workforce framework, often referred to as the NICE Framework, is arguably the most well-known cybersecurity education and training standard. It addresses the education and training needs of the cybersecurity workforce by providing common vocabulary for the field and a detailed list of cybersecurity Knowledge, Skills, Abilities, and Tasks (KSATs) for each identified cyber work role. While the NICE Framework is intended to be applicable to a wide range of cybersecurity workers in an organization, IT roles and IT KSATs are ultimately the focus of the competency recommendations provided. As IT and OT systems become increasingly connected and vulnerabilities associated with both increases, the need to extend the framework to incorporate ICS systems has begun.

INL in collaboration with academic and industry partners has endeavored to assist in the efforts to address the lack of a similar framework and KSATs for OT work roles. A major first step was INL's collaboration with Idaho State University (ISU) and La Trobe University (LTU) in a two-phased project resulting in the "Building an Industrial Cybersecurity Workforce: A Manager's Guide". This non-prescriptive document is a first step toward identifying the unique knowledge and job roles required of ICS professionals and establishing a capable workforce. NIST has recognized the value of this effort and has requested INL's participation in expanding the NICE Framework to incorporate OT roles and OT KSATs.

Lack of recognized OT job roles and associated KSATs has had a definite influence on the existing availability of OT-specific workforce training offerings. Years of research and development of education and training courses for CISA, DoD, and industry, collaboration with academic institutes, and interviewing students identified other potential influencers that appeared to be impeding the flow of the IT and OT cyber talent workforce pipeline. To validate INL's findings, we created a joint INL–ISU Industrial Cybersecurity Community of Practice (ICSCOP) recurring workshop and invited over 150 representatives from universities, Government entities, and industry experts to participate. Participants were provided presentations on two known cyber workforce issues: (1) Curriculum Standards for ICS cyber-related degree programs, and (2) ICS workforce development factors. The resulting group discussion by participants validated previously identified influencers and established working groups to address solutions. Influencers span IT and OT topics and included:

- First, standardized curriculum. There needs to be standard curriculum requirements for cyber-related degree programs, IT- and OT-focused, offered by academic institutes. For example, the requirements to attain a degree in cybersecurity varies from university, to university making is hard for employers to know the level of competency of any individual possessing such a degree and seeking

employment. Lack of standards also leave the individual unsure of their qualifications for jobs solely based on the degree.

- Second, employers do not understand the existing cybersecurity-related tasks their employees are responsible for in their daily jobs. This makes it impossible to know what each employee's cyber education and training requirements are or to create a roadmap for improvement. It also makes it difficult to identify if there is a need to hire additional staff to address unfilled cyber job roles. Employers require a holistic process that can assist with identifying the existing cyber job roles of their employees, identify potential personnel gaps, suggest individual cyber education and training roadmaps, and link the level of education of employees to the cyber "health" of the organization.
- Third, Human Resource (HR) departments do not possess the necessary tools to identify and hire the best candidate for a cyber-related job position. They are forced to use the same hiring methods as other positions within their business: Reviewing resumes and conducting interviews. Although academic institutes cannot create different degree programs tailored specifically for each individual business's needs, skills testing matched to standardized KSATs would assist employers with this issue and provide academic institutes a view of the most requested cyber skills by employers to adjust degree programs.
- Fourth, as mentioned previously, the pace of new cybersecurity emerging threats, new technology, vulnerabilities, etc., is faster than most of the existing board certification processes used by academic institutes to approve updated curriculum. This makes it harder for academic institutes to rapidly update materials and offer students programs with the most recent information. A central clearinghouse for approved new ICS cyber-related curriculum readily available for academic institutes to adopt if desired may be one solution.
- Fifth, closely aligned with the first influencer is the lack of availability of standardized hands-on or near-hands-on training apparatus for ICS cybersecurity education programs, especially in rural geographical areas. A shared repository of curriculum and capabilities provided in a hub-and-spoke regional model where all academic institutes benefit from a National repository of resources is the needed.
- Sixth, the existing workforce needs continuing education options from local academic institutes other than the time-consuming and expensive solution of employees obtaining another degree. The continuing education options must be trackable by individuals throughout their cyber careers and identify for employers the currency of the education the person has received. Academic institutes have begun establishing their own educational badge and/or credential systems. A recognized National standard for these systems is needed before employers will put stock in the validity of these necessary systems.

Outcomes from the ICSCOP workshops and working group meetings are not limited to validation of influencers impeding the flow of the cyber talent pipeline. INL is working with State and local government entities, academic institutes at all levels of education, and business around the State as collaborators and sounding boards of the workforce development solutions explored. The thought process to this approach is that if solutions can work in one State, they have a high probability of working in others.

An example of these activities is the Associate Lab Director for N&HS is a co-chairperson on a new task force led by the Idaho Department of Commerce. The purpose is to make Idaho the most secure State against cybersecurity attacks aimed at businesses, Governmental entities, institutions, and citizens which will substantially improve and protect our growing economy. Activities include coordinating, informing, and training Idahoans across the State as to safeguards and resources from the perspective of many experts and interested groups. Recommendations from the task force will inform the Governor, legislature, and other stakeholders on major cybersecurity threats and opportunities for Idaho. This effort can easily be replicated by other States desiring a collaborative approach to addressing cybersecurity issues.

Other efforts include Idaho National Laboratory (INL) in collaboration with industry, academia, and the science and research communities kicked off a multi-year Idaho Cyber Research Project (ICRP). This project is designed to apply existing solutions to some of the major influencers. A small army of interns (20 to 30) from Idaho universities and 2-year colleges are assisting INL staff by visiting organizations desiring assistance with cyber "health" issues and providing potential solutions. Solutions include using tools that can provide a cyber workforce evaluation resulting in cyber training paths validated by job roles for employees, assistance implementing new approaches to hiring cyber candidates and current employee cyber skills testing, cyber job posting solutions, consideration of apprenticeship opportunities, creating a workforce cyber competency profile for a business, and collaboration opportu-

nities with academic institutes desiring partnerships to improve cyber curriculum offerings to their sector-specific needs. Solutions that resonate with local entities and are validated will be briefed at future ICSCOP meetings to discuss options for adoption by a broader audience.

Finally, I would like to note that there are other issues facing the cyber workforce talent pipeline, but the ones listed are, in our opinion, the most problematic and biggest hinderances to a smoothly flowing talent pipeline. Many entities are working separately on solutions to the influencers I have outlined. This approach lends itself to creativity and flexibility with the multiple solutions offered to fit various entities needs; however, this approach can also lead to duplicative efforts and inefficient spending of scarce funds. We are seeing this issue arise with Federal and DoD entities. The CISA office of Cybersecurity Defense Education and Training (CDET) is uniquely poised to implement and manage National cyber workforce R&D programs along with education and training courses. CDET should be looked to as the lead office for all CISA workforce development efforts. DoD should establish a similar, joint office and directly collaborate with CDET for efficiency.

INL stands ready to assist as needed in this Nation's efforts to increase the cybersecurity posture of all citizens whether through workforce development and education or bringing to bear its ICS cybersecurity control systems experts, cyber researchers, engineers, and threat analysts.

I appreciate the opportunity to testify, and I want to thank you again for your attention to this very important issue for our Nation. I look forward to your questions.

Chairwoman CLARKE. I thank you, Mr. Ley, for your testimony.

Finally, I recognize Mr. Stier to summarize his statement for 5 minutes.

STATEMENT OF MAX STIER, PRESIDENT AND CEO, PARTNERSHIP FOR PUBLIC SERVICE

Mr. STIER. Thank you, Chairwoman Clarke and Ranking Member Garbarino. It is a real pleasure to have the opportunity to testify before you this morning on such an important issue.

Cybersecurity is so vital and our Federal Government is central to addressing this issue. My focus, as you indicated in the summary, of the Partnership for Public Service will be on the Federal work force. We are a nonpartisan, nonprofit organization really focused on better Government for a stronger democracy. We have been working on the issue of cyber for some time now.

Just to give one stat that helps demonstrate how big the problem is, if you look at the cyber work force in the Federal Government right now, under 6 percent of it is under the age of 30. So to be real clear, it is just extraordinary. There is no generational diversity more broadly.

There are five reasons for this. The first is that the Federal Government's brand is damaged. Government shutdowns, hiring freezes, negative rhetoric, political interference in science, all these things have tarnished the brand. Second, the opportunities for young people to serve are hidden and scarce. Again, a devastating statistic. Just 4 percent—4 percent of new hires are drawn from Federal programs employing current students and recent graduates. So Government rarely gets talent coming in that is young, bluntly. No. 3, the hiring process is broken and the barriers to entry are many—could spend all 5 minutes on this, and I am going to pass unless you want more detail later—100 days-plus to hire people and the assessment processes are broken. Very importantly and often overlooked, this is No. 4, we are not retaining the talent that we get. So if you look at those full-time employees under the age of 30 who are leaving Government, three-quarters of them are

leaving within 2 years. So if you do everything right on the front end and you don't address the retention issue, you actually don't solve the problem. Fifth, critically, the diversity is bad across the Federal work force, but it is much, much worse in the cyber arena.

Now, cybersecurity has been on the GAO high-risk list since 1997. we need to do more than admire this problem. Ranking Member Garbarino, I loved your point, let us have some concrete things to do. I am going to give you 10 of them.

First and foremost, most important, we need to create higher expectations for the leadership in Government, and that includes, bluntly, Congress as well. We need leadership to pay attention and to see it as their responsibility to own getting the right talent into Government. By and large they don't do that and it is a big problem.

No. 2, we need the leaders in Government to actually have a very different level of understanding around technology. I am not talking about obviously the CIOs and the CTOs. The general program leadership more broadly in the world that we live in today has to have a sophistication and fluency in technology that is often missing. They need to be upscaled or different people need to be brought in.

Third, and equally important, we need more sustained leaders. Right now a Senate-confirmed appointee lasts only 2 years on average. It is impossible, bluntly, to make a difference on these management issues like cyber without a longer-term tenure for leaders. So a very concrete example, Secretary Granholm wants to have a CESER career leader in there rather than a political appointee. That is very smart.

No. 2, we need to utilize innovative talent models like our cyber talent initiative. Happy to describe that in greater detail.

No. 3, we need to promote the Government mission. People will come to Government if they understand they are serving the American people. NASA does a great job. They have a custom-built career website that includes videos of what they do. We produce a program called a Service to America Medals. We need to be able to highlight the great things people can do if they are in Government.

No. 4, we have got to improve the recruiting and hiring to begin with. We had the National Commission on Military National Public Service. They did a fantastic job. Lots of recommendations that are ready for legislation now and they should be done. We should have exit interviews of those in the cyber fields so we are understanding why we are not holding onto talent that we need.

No. 5, we need to get more young people in Government. Here this is basic strategy. Student internships ought to be the primary entry hiring for Government. They are not right now. They need to be paid internships or else we are not going to get the diverse talent.

No. 6, we need to overhaul the pay system more broadly in Government and certainly around cyber. Know that this pay system in Government was designed in 1949. It is not sufficiently market-sensitive. That is a real problem.

Seven, we have got to invest in the H.R. work force or you won't have these people coming in. We need an enterprise strategy.

Eight, we need to embrace a culture that has technology and innovation collaboration that is central. That is a leadership issue. I mentioned DEI as being critical in this work force strategy.

Ten, coming back around to the leadership side, we need continued oversight from this committee, we need to see this as an annual hearing, we need to see you visiting agencies that are doing well, and we need you looking out for the Government brand.

As fast as I can talk. Look forward to questions.

[The prepared statement of Mr. Stier follows:]

PREPARED STATEMENT OF MAX STIER

JULY 29, 2021

INTRODUCTION

Chairwoman Clarke, Ranking Member Garbarino, and Members of the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation, thank you for the opportunity to appear before you today to discuss the importance of building a robust cybersecurity talent pipeline.

The Partnership for Public Service is a non-partisan, non-profit organization dedicated to inspiring public service and increasing the efficiency and effectiveness of the Federal Government. The Partnership was founded on the premise that any organization's best asset is its people.

Cybersecurity, a critical element of any organization's resilience, has been indispensable to the Federal Government's response to the COVID–19 pandemic. Early in the pandemic, security considerations moved to the forefront as more employees than ever before worked and accessed agency information networks remotely and used digital tools to continue operations and service delivery. As the Federal Government thinks about the future of work, it is clear that cybersecurity will remain at the forefront. And, of course, there are moments of crisis in securing the Nation's cyber infrastructure—the SolarWinds cyber attack in 2020 and the Colonial Pipeline hack in May 2021 illustrate the importance of having Federal cyber experts who can respond quickly to an increasingly sophisticated threat landscape.

Although these cyber attacks shine a fresh spotlight on the country's vulnerabilities, cybersecurity has been identified as a GAO High-Risk List area since 1997.[1] Despite being on the list for 24 years, there remains a Nation-wide shortage of highly-qualified cybersecurity specialists, and the Federal Government has fallen behind in the race for this talent. Amidst the growing demand for cyber professionals, agencies have struggled to recruit, hire, retain, and train workers in the cybersecurity field. Many of the personnel issues confronting the cybersecurity workforce are endemic in the Federal system that makes recruiting and retaining the best and brightest talent in any career field a formidable challenge. To protect the country against current and future threats, Congress must focus on revitalizing and investing in the Federal cyber workforce.

The Partnership offers a variety of programs that allow us to work with Federal employees to strengthen their leadership skills, prepare them to build strong teams and work across organizational boundaries. We also work with agencies on issues such as attracting top talent, engaging and supporting their workforce, and fostering innovation. For example, our cross-sector Cybersecurity Talent Initiative[2] is a partnership with MasterCard, Microsoft, and Workday that provides students in cybersecurity-related fields with public and private-sector work experience. This program guarantees students a 2-year placement at a Federal agency with cybersecurity needs and provides agencies with capable talent to address current and emerging challenges. Through these initiatives, we help Federal leaders and agencies achieve better outcomes for the people they serve.

For the past decade, the Partnership's research has highlighted strategies and opportunities for Government to build a more capable cyber workforce. For instance, our 2009 "Cyber In-Security" report outlines factors hampering Government's ability

[1] Senate Committee on Homeland Security and Governmental Affairs, "GAO's 2021 High Risk List: Addressing Waste, Fraud, and Abuse," March 2, 2021. Testimony from Eugene L. Dodaro, Comptroller General of U.S. Government Accountability Office. Retrieved from *https://www.hsgac.senate.gov/gaos-2021-high-risk-list-addressing-waste-fraud-and-abuse.*

[2] Cybersecurity Talent Initiative. Retrieved from *https://cybertalentinitiative.org/*.

to build an efficient and effective cybersecurity workforce.[3] Our 2015 supplementary report, "Cyber In-Security II," outlines key findings and strategies to help Government build a capable cyber workforce and close the Federal talent gap.[4]

CHALLENGES FACING THE FEDERAL CYBER WORK FORCE

Unpacking the data on the Federal cybersecurity work force reveals different stories across the Government. There are areas of growth, including in Government-wide totals—the number of full-time Federal cyber employees increased by 7.85 percent between September 2016 and September 2020. Over the same period, the Federal work force overall increased by 3.66 percent.

However, there are concerning trends in other areas of the cyber workforce. For example, some agencies saw declines in full-time employees—the Department of Agriculture's cyber workforce decreased from 3,300 employees in September 2016 to 2,700 in September 2020, while at the Department of Labor it decreased from 750 to 660 employees in the same time frame.[5]

Government also faces challenges in recruiting, hiring, and retaining a cyber workforce that looks like the American public. For example, 50.8 percent of the U.S. population identifies as female;[6] however, in September 2020, just 25.4 percent of the full-time Federal cyber workforce identified as female, compared to 43.2 percent Government-wide.

The Federal cybersecurity workforce is also older than the U.S. labor force. The percent of full-time cyber employees under the age of 30 steadily increased from 4.1 percent to 5.7 percent between September 2014 and September 2020; however, this still lags behind the almost 20 percent of the employed U.S. labor force in 2020 that is under age 30.

To revitalize the cyber workforce, the administration and Congress must address both immediate and long-standing problems. Key data points from the overall Federal workforce signal the urgent need for attention to this vital National asset. These trends are not new but will be harder to fix the longer we wait:

- In the Federal IT workforce, there are 16 times more employees over the age of 50 than under age 30.
- Roughly one-third of full-time employees on board at the beginning of fiscal 2019 will be eligible to retire by the end of fiscal 2023.
- Use of the Federal Pathways intern program, which should be a main pipeline into Federal service, has plummeted. According to the fiscal 2020 budget request, the number of new hires of student interns fell from 35,000 in 2010 to 4,000 in 2018.[7]
- Of the full-time employees under 30 who voluntarily quit Federal service in fiscal 2019, over 73 percent did so with less than 2 years of Federal tenure, suggesting that many young people do not have a positive work experience in the Federal Government or lack sufficient incentives to stay in Federal service.
- Data also shows major diversity challenges in the Federal workforce, which grow even greater at the higher echelons of service. For example, only 35.5 percent of the career Senior Executive Service are female, and only 22.7 percent of the career SES are people of color.
- The 2020 Best Places to Work in the Federal Government® [8] employee engagement score was 69 out of 100, lagging behind the private sector by more than 8 points and suggesting that more can be done to cultivate a highly engaged, high-performing Federal workforce.
- It takes the Government an average of 98 days to bring new talent on board—more than double the time in the private sector.[9]

---

[3] Partnership for Public Service, "Cyber In-Security," July 2009. Retrieved from *https://ourpublicservice.org/publications/cyber-in-security-strengthening-the-Federal-cybersecurity-workforce/*.

[4] Partnership for Public Service, "Cyber In-Security II," April 2015. Retrieved from *https://ourpublicservice.org/publications/cyber-in-security-ii-closing-the-Federal-talent-gap/*.

[5] Statistics on Federal employees are drawn from Office of Personnel Management FedScope data on the Federal workforce unless indicated otherwise.

[6] U.S. Census Bureau. Retrieved from *https://www.census.gov/quickfacts/fact/table/US/PST045219*.

[7] "Analytical Perspectives, Budget of the U.S. Government, Fiscal Year 2020," March 18, 2019, p. 77. Retrieved from *https://www.govinfo.gov/content/pkg/BUDGET-2020-PER/pdf/BUDGET-2020-PER.pdf*.

[8] Partnership for Public Service, Best Places to Work in the Federal Government®. Retrieved from *https://bestplacestowork.org/*.

[9] Office of Personnel Management, "OPM Issues Updated Time-to-Hire Guidance," February 2020. Retrieved from *https://www.opm.gov/news/releases/2020/02/opm-issues-updated-time-to-hire-guidance/*.

- About 83 percent of major Federal departments and agencies struggle with staffing shortages and 63 percent report gaps in the knowledge and skills of their employees.[10]
- According to the Survey on the Future of Government Service,[11] just 32 percent of respondents say their agency has a strategic recruitment plan that is aligned to its workforce needs.

THE IMPORTANCE OF STRENGTHENING GOVERNMENT'S CYBER WORKFORCE

Federal jobs offer mission-driven work with opportunities to help solve the biggest challenges facing our Nation. Our Government needs cyber talent to secure our National security and economic interests, and help the country rise to the significant challenges of the day and prepare for what lies ahead. In particular, the dearth of young civil servants represents a lost opportunity for our Federal Government as well as the Nation's young professionals.

The Federal Government not only needs to work harder to recruit and hire great talent, but also create an environment that retains high-performing employees. Fundamental reforms to the Government's antiquated pay and classification system—or more targeted personnel systems, such as the DHS cyber personnel system—would better equip the Government to compete for cyber talent. Even within the constraints of the Federal pay system, though, our Government can pursue multiple strategies to make the Federal Government the employer of choice not only for entry-level talent but also for mid- and senior-level talent.

There are many reasons why Government is failing to recruit and retain talent, especially young people, and the problems are deep-seated:

The Federal Government's brand is damaged.—Government shutdowns, hiring freezes, and negative rhetoric have hurt the image of Government and the people who serve. An Axios Harris poll in March 2019 examined the reputation of America's 99 most high-profile companies and the Federal Government, and the Government ranked dead last.[12] That was before a pandemic further eroded public confidence in Government.

Opportunities for young people are hidden and scarce.—Many students do not know about compelling career opportunities in Government or how to apply for them. In addition, Government hiring processes have historically shown a disproportionate preference for experienced professionals, limiting opportunities for promising young talent. For instance, internships are underused across the Federal Government and just 4 percent of new hires are drawn from Federal programs employing current students and recent graduates. An added challenge for the cyber community is that candidates often find it difficult to enter the Federal workforce due to poor advertisement of available cyber opportunities in Government. This is largely due to the antiquated way these jobs are classified and outdated position descriptions that do not accurately depict the skills and knowledge necessary for the role.

Barriers to entry abound for job candidates. An unintuitive on-line jobs portal in USAJOBS, a 70-year-old compensation system, and a time-to-hire average of nearly 100 days all make it difficult for Government to attract top talent. Government may always struggle to match private-sector salaries, but it must do better on multiple human resource fronts in the competition for mission-critical talent.

We are failing to adapt to the needs of a more mobile workforce.—Our Federal personnel system is geared to the model of the lifetime Federal employee. We value and need those who want to dedicate their whole careers to Federal service. But we also must seize opportunities to recruit those who want to serve for shorter durations, especially as younger workers increasingly want more mobility in their careers. Just 35 percent of millennials expect to stay with their current employer for 5 or more years, but there were notable correlations between those who did plan to stay and those who believe their employers perform well on issues related to fi-

---

[10] Office of Personnel Management, "2018 Federal Workforce Priorities Report," February 2018. Retrieved from *https://www.opm.gov/policy-data-oversight/human-capital-management/Federal-workforce-priorities-report/2018-Federal-workforce-priorities-report.pdf*.

[11] "Survey on the Future of Government Service," October 13, 2020. The survey is a collaborative effort by the Partnership for Public Service, the Princeton School of Public and International Affairs at Princeton University, the Center for the Study of Democratic Institutions at Vanderbilt University and Georgetown University. Retrieved from *https://ourpublicservice.org/publications/survey-on-the-future-of-government-service/*.

[12] The Harris Poll, "Axios Harris Poll 100," 2019. Retrieved from *https://theharrispoll.com/axios-harrispoll-100-2019/*.

nancial performance, community impact, talent development, and diversity and inclusion.[13]

Undergirding these challenges is the need for a heightened commitment to diversity, equity, and inclusion.—While the Federal Government outperforms many private-sector organizations on this front, there is room for improvement in Federal leadership ranks. Among career leaders in the Government's Senior Executive Service (SES), just 36 percent are female and only 23 percent identify as people of color. And among SES leaders in STEM, just 26 percent are female and only 18 percent identify as people of color. Federal agencies need to do more to provide and promote opportunities to underrepresented communities and ensure that our Government mirrors the people it serves.

Altering the status quo will not be easy but it will be critical to the Nation's future. And this moment in time offers a rare convergence of opportunity: A Federal workforce which has dramatically changed the way it works over the past year and is primed for adaptation amid the staggering health, social, and economic challenges it must take the lead in tackling; and the rise of Generation Z, which is technologically adept and hungry to make a difference.

The past year has shown the dedication, resiliency, and resourcefulness of the Federal workforce. At many agencies, most Federal employees shifted quickly to telework as the pandemic spread, while others bravely remained on the front lines in jobs that cannot be performed remotely. On all fronts, Federal workers have found innovative ways to serve the people during the pandemic. Thus, out of crisis comes opportunity. We have a once-in-a-generation moment to transform the workforce and the way it works, and to inspire Americans to enter public service.

Both the world and the workplace are rapidly changing. In the post-pandemic era, we must not go back to the old ways of doing business when the new ways make more sense. We should seize this moment to modernize the ways in which Government operates, which in many instances are predicated on laws and practices that are decades old and out of sync with today's fast-paced digital economy and invest in a cybersecurity workforce for the future.

SOLUTIONS FOR BUILDING THE CYBER TALENT PIPELINE: WHAT CAN CONGRESS DO?

Here are ten ways that Congress can accelerate this revitalization and transformation of the Federal cyber workforce:

(1) Create high expectations for Federal leaders.

A transformation of the workforce and how Federal employees do their jobs will not be possible without also reimagining leadership in the Federal Government. Good leaders motivate and advocate for their employees, build trust and create the conditions necessary for employees to perform at their best. The civilian side of Government should take a lesson from the military side, where people are viewed as an asset, not a cost, and where investments in leadership development are critical to the strategy for success.

In 2019, the Partnership developed the Public Service Leadership Model,[14] recognizing the unique nature of leadership in Government, centered on stewardship of public trust and commitment to public good. We believe this model should be the standard for leaders—both career and political—across the Federal Government. The model identifies the core values that leaders must prioritize and the critical competencies they must master to achieve their agencies' missions and desired impact. These include setting a vision, empowering others and being accountable for results. We were proud to create this model with a nonpartisan group of distinguished leaders from across sectors, and in the months to come we hope to work with Congress, the Executive branch and others to improve and measure overall leadership effectiveness.

Congress also should hold political and career Federal leaders accountable not only for owning policy but also for the organizational health of their agencies. In many cases, agencies and bureaus could benefit from career executives at the helm—nonpartisan, professional leaders who can provide needed stability and deep expertise. An example of this is the Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER), which is currently helmed by a career civil servant. Our Government has over 4,000 politically-appointed positions, with roughly 1,200 of them subject to Senate confirmation, and the process for selecting, vetting, and appointing them is complex, inefficient, and time-con-

[13] Deloitte, "The Deloitte Global Millennial Survey 2020," June 25, 2020. Retrieved from *https://www2.deloitte.com/global/en/pages/about-deloitte/articles/millennialsurvey.html.*

[14] Partnership for Public Service, Public Service Leadership Model. Retrieved from *https://ourpublicservice.org/our-work/public-service-leadership-model/*.

suming. We encourage Congress to consider reducing the number of political appointees and creating more opportunities for career experts to lead.

In addition to taking ownership of the health of the workforce, political and career programmatic and policy leaders in Government today must also have a familiarity with technology and cybersecurity issues in order to focus on key priorities and make informed choices. That's why the Partnership created the AI Federal Leadership Program in 2019. This 6-month, complimentary program is meant to help Federal leaders (specifically members of the SES) better understand the needs and opportunities around artificial intelligence, and prepare them to integrate this technology with policy and program implementation. This program is another cross-sector effort with technology leaders, including Microsoft, Google, and the Ford Foundation.

With respect to the workforce, Congress should hold political appointees responsible for recruiting and retaining highly-qualified talent, developing future leaders, engaging employees, and holding subordinate managers accountable for addressing performance. Congress should urge agency leaders to use the annual Federal Employee Viewpoint Survey and the Best Places to Work in the Federal Government® rankings to drive better results in their agencies. Employee engagement is not just about happy employees. Higher scores in employee engagement equate to better performance and higher-quality service, which in turn become valuable recruiting tools. For example, in a recent analysis of performance data from nearly 150 Department of Veterans Affairs hospitals across the country, the Partnership found that higher patient satisfaction, better call center performance and lower nurse turnover were all associated with a more satisfied and committed workforce.[15]

Congress and the administration should also embrace the bold goal of closing the over 8-point gap between the Government and the private sector in the Best Places to Work in the Federal Government® engagement index, and even increasing the Federal score over the private-sector score. The Government has a powerful asset in having a mission-driven workforce. This purpose-driven work, if combined with excellent leadership, will lead to much more engaged employees and better outcomes for the American public.

(2) Utilize innovative talent models.

To attract talent at all levels, Congress and the administration should work together to create new and innovative pathways—and expand existing ones—for diverse mission-critical talent to join public service through fellowships, talent exchanges, and service corps.

In 2019, the Partnership collaborated with Mastercard, Microsoft, Workday, and a dozen Federal agencies to establish the Cybersecurity Talent Initiative, which aims to build the next generation of cyber leaders for our country. This innovative cross-sector opportunity enables recent graduates to spend 2 years working for and receiving training in the Federal Government in a cyber-related position. At the end of 2 years, they will have an opportunity to apply for a position with one of the corporate partners and, if hired, will be eligible to receive student loan assistance up to $75,000 from their private-sector employer. This model is the first of its kind. The inaugural class of eight future cybersecurity leaders brings a variety of academic and professional experience to five Federal agencies, and we anticipate placing at least 25 participants across nine Federal agencies and components for the second cohort.

One benefit of these efforts is that we are educating young people about cyber careers across sectors and helping them learn about organizations and missions they may have never heard of before. Other Federal programs like the U.S. Digital Service, 18F, and Presidential Innovation Fellows allow "technical tours of duty" with the Federal Government and are unique in helping promote and respond to an increasing desire for the next generation to be more mobile in their careers. The programs provide a model for filling other "hard-to-fill" positions in Government.

(3) Promote Government's mission.

Both the world and the workplace are rapidly changing. Our Government needs a new generation of young people to serve in a data- and technology-driven environment, with expertise in such sectors as cybersecurity, technology, engineering, finance, and health care. Making the Federal Government an "employer of choice" requires greater awareness by the Government of what employees want in the workplace, coupled with improved public perception of opportunities in Federal service.

---

[15] Partnership for Public Service, "Employee engagement is more than just a survey," March 2, 2020. Retrieved from *https://ourpublicservice.org/blog/employee-engagement-is-more-than-just-a-survey/*.

As the Federal Government struggles to attract students and recent graduates, it is clear that more must be done to improve the Government's "brand." Government shutdowns, hiring freezes, and negative rhetoric damage the image of Government and the people who serve.

The Federal Government, because of budget constraints, will always have a hard time competing with the private sector on pay, but agencies almost always have an advantage in offering employees a sense of mission. Our Best Places to Work® rankings regularly show that the match between employee skills and agency mission is a key driver of employee engagement, second only to effective leadership. Too often, though, Federal job announcements are dry, confusing, and fail to inspire. The Partnership has identified bright spots in marketing, such as NASA's custom-built career website, which supplements USAJOBS and showcases their mission, including through videos from current employees sharing their stories.[16] NASA understood that, to attract professionals in STEM fields, the agency needed to set itself apart from other employers by focusing on its unique mission and impact. Other agencies, such as the Department of the Interior, leverage social media platforms to promote their missions and the work of their agency.

The Federal Government needs to do more to showcase the incredible array of professional opportunities it offers and to recognize the accomplishments and innovation of the current workforce. Without compelling and shared stories of success in Government, Government will struggle to become an employer of choice for the tech-savvy, forward-looking talent that it needs to attract.

This subcommittee can also play an important role in encouraging Congressional colleagues to recognize the successes of the Federal workforce. Federal employees are often blamed for policy failures, and rarely acknowledged when things go right. One way to revitalize the workforce is simply to change the tone and get away from the demeaning rhetoric that frequently characterizes discussion of the Federal workforce. Political leaders should celebrate outstanding contributions, such as the remarkable achievements of the nominees and winners of the annual Service to America Medals [17] and the Presidential Rank Awards.

(4) Improve recruiting, hiring, and retention.

Congress should start the hard process of updating the legal framework for the civil service, much of which dates back to laws passed in 1949 and 1978. The Federal Government needs cybersecurity experts, doctors, economists, and emergency response specialists, but we have a personnel system designed for phone operators. The antiquated system is an impediment to the Government's ability to meet the needs of today's interconnected, technology-driven world and prepare for the challenges of the future. A Government-wide initiative could help agencies improve the hiring process so they can more easily attract, assess, hire, and on-board highly-qualified applicants. This effort should include simplifying and demystifying the application processes, including the USAJOBS portal.

As a starting point, Congress should enact the civil service recommendations of "Inspired to Serve," the final report of the National Commission on Military, National, and Public Service.[18] On a bipartisan and consensus basis, and after studying the Federal civil service for over 2 years, the Commission issued last year a bold and thoughtful set of recommendations for improving talent management, including proposals to make Federal hiring more efficient. We urge Congress to move forward on a bipartisan basis as quickly as possible to enact these proposals. Some key Commission recommendations—and ideas the Partnership has long supported—include:

- Establishing a civilian cybersecurity reserve program, as proposed in the bipartisan Civilian Cyber Security Reserve Act (H.R. 2894).
- Allowing agencies to appoint Federal employees who have successfully completed reskilling programs to positions in their new field without the employee having to move to a lower grade level, as proposed by the bipartisan Facilitating Federal Employee Reskilling Act (S. 1330).[19]
- Amending the criteria for direct hire authority to enable agencies to use this authority when they face a shortage of highly-qualified applicants.
- Expanding direct hiring authority for students and recent graduates.

---

[16] Partnership for Public Service and Salesforce, "Tech to Hire: Transforming Federal H.R. Beginning with Recruiting and Hiring," October 3, 2018. Available at *https://ourpublicservice.org/wp-content/uploads/2018/10/TechtoHire.pdf.*

[17] Service to America Medals. Retrieved from *https://servicetoamericamedals.org/.*

[18] National Commission on Military, National and Public Service, "Inspired to Serve," March 25, 2020. Retrieved from *https://inspire2serve.gov/reports.*

[19] This legislation was included in S. 1260, the U.S. Innovation and Competition Act of 2020, which passed the Senate in June.

- Modernizing the veterans' preference rules, which are currently confusing for both agencies and veterans alike.
- Improving the Pathways programs, which include the Presidential Management Fellows and intern and recent graduate programs.

The Government not only needs to work harder to recruit and hire great talent, but also to retain it. Even within the constraints of the Federal pay system, the Government can pursue multiple strategies to make the Government the employer of choice not only for entry-level talent but also for mid- and senior-level talent. When people do leave Government, agencies should be collecting data on their reasons for departing or taking another job. Currently, a Government-wide exit survey exists only for the SES. Data on why people leave Government will be instrumental in helping agencies better recruit and retain the next generation. The surveys would be particularly useful in understanding why almost half of people who quit working for the Federal Government leave within 2 years.

(5) Get young people in Government.

Today's college students are interested in making a difference, but those considering the Federal Government as a place where they can do so face challenges in getting hired. Programs that Congress should reinvigorate include the Pathways programs, which provide younger, early career talent with exposure to and positive experiences working in Government. Needed improvements include ensuring internships are paid and easing agencies' ability to convert interns into full-time positions. In addition to lifting the caps on the expedited hiring authority for students and recent graduates, Congress should also consider an ROTC-like program for Federal service and encourage agencies to recruit on campuses.

The need to improve the hiring process is especially urgent for cybersecurity jobs, where Government faces stiff competition for talent with the private sector. The Federal Government's antiquated hiring system is not designed to compete at the speed of private-sector companies who can actively recruit and quickly hire young STEM and cyber talent. Dr. Elizabeth Kolmstetter, NASA's Director of Talent Strategy and Engagement, gave an example of one Texas A&M student who met a SpaceX recruiter and was offered a job the same day, finalized the offer over the weekend and moved to California the next week to begin work.[20] Kolmstetter also noted that in fiscal year 2018 about 61 percent of NASA's engineering vacancies, 87 percent of scientist vacancies, and 86 percent of mathematics vacancies had fewer than three qualified (not most qualified)[21] applicants. The talent is out there, and Government's mission remains more compelling than ever, but agencies are losing out because the Federal hiring system isn't nimble enough to compete with the private sector.

(6) Overhaul the pay and classification system.

The Government's 1949 pay and classification system was designed for clerical workers, not for the highly professional, specialized skills that are needed in today's civil service. The lack of an occupation-specific, market-based compensation system is particularly damaging to the ability of the Federal Government to recruit and retain scientists, many of whom have far more lucrative opportunities in the private sector.

The OPM Handbook of Occupational Groups and Families contains 407 separate job series. The sophisticated cyber, IT, data science and STEM skills that the Government badly needs were barely envisioned when the system was created. We need broader pay-banding that allows agencies the flexibilities to set more market-based, occupational-specific salaries. Unique pay systems like that created under the authority of the Financial Institutions Reform, Recovery, and Enforcement Act (FIRREA) of 1989 are an acknowledgement that a rigid pay system does not work. While the Federal Government will never be able to match private-sector salaries for many positions, broader pay bands would enable agencies the flexibility to attract the most critically-needed talent.

---

[20] Testimony before the National Commission on Military, National, and Public Service, "Public Service Hearing: Critical Skills and Benefits," May 15, 2019. Retrieved from *https://inspire2serve.gov/sites/default/files/2020-09/Kolmstetter%20Testimony__Public%20Service%20Hearing__Critical%20Skills%20and%20Benefits.pdf*.

[21] Qualification standards are "a description of the minimum requirements necessary to perform work of a particular occupation successfully and safely," according to OPM.

The Partnership's report, "Building the Enterprise: A New Civil Service Framework,"[22] laid out a new pay-setting process for the Federal workforce. The modernized pay system would establish broad pay bands for employees rather than rigid grades, better align salaries and benefits on an occupation-by-occupation basis, set salaries based on those comparisons and give agencies the flexibility to bring talent in at the appropriate salary level. While this is a long-term effort, allowing market-based pay for specific mission-critical occupations in the near term is a place to start and would help attract and retain needed talent. Again, the final report of the National Commission on Military, National, and Public Service also endorses a comprehensive modernization of the entire Federal talent management system.

The Partnership's recent studies reinforce the need for investment in the Federal human resources workforce. For example, our "State of Renewal" report lays out recommendations for improving the State Department's talent management life cycle over 6 to 12 months, without the need for any additional legislation, as well as changes that will take longer and require Congressional action. Our report "Time for Talent: Improving Federal Recruiting and Hiring"[23] lays out practical approaches that agencies can take within the existing system to attract mission-critical talent. And in "Rapid Reinforcements: Strategies for Federal Surge Hiring,"[24] we identified strategies that can help agencies when faced with circumstances that require a rapid growth in the workforce, such as National emergencies, large-scale attrition, new mission requirements, or the need for emergent skills.

(7) Invest in the H.R. workforce.

Agencies cannot move forward on these recommended strategies, however, unless their human resource offices have the requisite skills, capacity, and tools. There are outstanding and innovative H.R. professionals across the Government, but there are also skills gaps in their offices. They are often overwhelmed by responsibilities and the complexities of Federal human capital law. Often, H.R. specialists are not familiar with the authorities they have available to them, and do not have the technologies, data, and analytical skills that would better enable them to recruit and hire while also engaging in strategic workforce planning for the future.

Congress should jump-start efforts to increase the skills and professionalism of the Federal H.R. community by requiring OPM to start providing technical training to H.R. specialists again, conducting a review of overall training needs and how those needs can be met, and funding IT needs of the H.R. community. Congress should also ensure that agencies undertake strategic workforce planning and make sure that Chief Human Capital Officers have a voice in the strategic and budget planning processes so that agency leaders will be informed of the H.R. needs necessary to carry out their policies and programs.

(8) Create a workforce culture that embraces technology, innovation, and collaboration.

Our recent report "Resilient: Keeping Your Wits—Workforce, Innovation, Technology, Security—About You,"[25] summarizes a survey of 300 Federal leaders and a series of roundtable discussions on the lessons of the pandemic. A key takeaway is that an agile workforce, cutting-edge cybersecurity, modern technologies, and continual innovation are all interdependent in creating resiliency in the Federal Government. Also, when asked what a resilient Federal Government looks like, more respondents linked resiliency to an agile workforce than the other issue areas discussed in the report.

The success of the Federal workforce depends not only on the quality of its talent and its leaders, but also on a culture where employees are encouraged to try new ideas and make smart technology investments. The new workplace environment must also involve more collaboration between Federal, State, local, and Tribal governments and the private and non-profit sectors.

---

[22] Partnership for Public Service, "Building the Enterprise: A New Civil Service Framework," April 10, 2014. Retrieved from *https://ourpublicservice.org/publications/building-the-enterprise/*.

[23] Partnership for Public Service, "A Time for Talent: Improving Federal Recruiting and Hiring," August 26, 2020. Retrieved from *https://ourpublicservice.org/publications/a-time-for-talent/*.

[24] Partnership for Public Service, "Rapid Replacements: Strategies for Federal Surge Hiring," October 29, 2020. Retrieved from *https://ourpublicservice.org/publications/rapid-reinforcements-strategies-for-Federal-surge-hiring/*.

[25] Partnership for Public Service, American Council for Technology and Industry Advisory Council, and Meritalk, "Resilient: Keeping Your Wits—Workforce, Innovation, Technology, Security—About You," January 25, 2021. Retrieved from *https://ourpublicservice.org/publications/resilientkeeping-your-wits-about-you/*.

Recognizing that revitalizing the Government requires attention to leadership and stewardship, talent, innovation and technology, and collaboration, the Partnership's "Roadmap for Renewing the Federal Government,"[26] launched last fall, describes the challenges the Government faces in each of these areas, bright spots showing improvements, and needed solutions. The Roadmap provides a list of actions that the Biden administration and Congress can take to begin laying the groundwork for renewing the Federal Government, and the issue pages on the website summarize proposals that we believe should have the support of both Congress and the administration.

(9) Make diversity, equity, and inclusion a central part of workforce strategy.

A commitment to diversity, equity, and inclusion must be a cornerstone in the transformation of how the Government recruits, hires, develops, and retains talent.[27] The Partnership hears consistently from current and former agency leaders that it is critical to address this issue in the scientific and technical community. This commitment ultimately leads to higher organizational performance by ensuring the door is open for top talent and by enabling new and creative ways of thinking that empower better decision making. Also, a Government that better reflects its people also will increase public trust in our democratic institutions.

President Biden has issued a memorandum prioritizing diversity, equity, and inclusion as a National security imperative, in order to ensure that critical perspectives and talents are represented in the entire National security workforce.[28] Congress should support these efforts, and should help ensure that diversity, equity, and inclusion are in the DNA of every department and agency in the Federal Government.

(10) Continue oversight and get to know Federal employees.

The subcommittee today is helping to identify challenges and opportunities facing the Federal cyber workforce. We encourage you to make this hearing an annual occurrence. The subcommittee could follow up by holding a hearing on agencies and subcomponents that are doing well with cyber recruiting, hiring, and employee engagement to help celebrate success and encourage replication.

Members of Congress should also get out to visit agencies and their employees and hear from those on the front lines. Visiting Federal employees where they work, whether at headquarters or in the field, is one of the best ways to understand both the deep challenges facing the Federal workforce and the incredible work that the Federal Government does on behalf of the American people every day. Better yet, the vast majority of Federal employees are located outside of Washington, in every State and Congressional district, so they are also your constituents.

Finally, policy makers should remember that they are stewards of Government's brand. How Members of Congress discuss public servants matters, especially when communicating with the next generation. When speaking to students—in formal settings like commencement speeches or simply in conversations with constituents—take the opportunity to share Government's unique, mission-focused work and the vital role of Federal employees.

CONCLUSION

Congress has an opportunity right now to further drive bold cybersecurity reforms to keep pace with the evolution of technology and meet the challenges of today and tomorrow.

For this reason, we want to commend the bipartisan effort made by this subcommittee to pass legislation that will strengthen the Nation's cybersecurity.[29] The

---

[26] Partnership for Public Service, "Roadmap for Renewing the Federal Government. Retrieved from *https://ourpublicservice.org/roadmap-for-renewal/*.

[27] For example, see Jennifer Miller, "For young job seekers, diversity and inclusion in the workforce aren't a preference. They're a requirement," Washington Post, February 18, 2021. Retrieved from *https://www.washingtonpost.com/business/2021/02/18/millennial-genz-workplace-diversity-equity-inclusion/*.

[28] President Joseph R. Biden Jr., "Memorandum on Revitalizing America's Foreign Policy and National Security Workforce, Institutions, and Partnerships," February 4, 2021. Retrieved from *https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/04/memorandum-revitalizing-americas-foreign-policy-and-national-security-workforce-institutions-and-partnerships/*.

[29] House Committee on Homeland Security, "House Passes Thirteen Bipartisan Homeland Security Bills, Including Cybersecurity Grant Program," July 1, 2021. Retrieved from *https://homeland.house.gov/news/legislation/house-passes-thirteen-bipartisan-homeland-security-bills-including-cybersecurity-grant-program.*

State and Local Cybersecurity Improvement Act (H.R. 3138)[30] introduced by Chairwoman Clarke and Ranking Member Garbarino will provide funding to ensure State, local, Tribal, and territorial governments are securing their cyber environments. The Cybersecurity Vulnerability Remediation Act (H.R. 2980)[31] introduced by Rep. Jackson Lee will allow the Department of Homeland Security to continue mitigating cybersecurity weaknesses that exist due to insufficient software or hardware. And the CISA Cyber Exercise Act (H.R. 3223)[32] introduced by Rep. Slotkin will strengthen the agency's ability to fulfill its intended mandate by establishing a program to assess and review CISA's preparedness and resilience to cyber attacks. These measures will build upon work from the previous Congress to improve Government's cyber capabilities and ensure the effectiveness of CISA and other cyber components.

We also applaud the introduction of the Federal Rotational Cyber Workforce Program Act by Senators Peters, Rosen and Hoeven in the Senate (S. 1097)[33] and Representatives Khanna and Mace in the House (H.R. 3599).[34] These bills would help the Federal Government better train and retain cybersecurity professionals and provide Federal employees with professional development opportunities that ensure the Nation's future cyber needs are met.

Thank you again for holding this hearing. Building a robust cyber talent pipeline is a complex but necessary endeavor, and this testimony only scratches the surface of the efforts that are needed across the Executive and Legislative branches. We look forward to working with you and your staff as you move forward with your legislative and oversight agenda for the Federal cyber workforce in the 117th Congress.

Chairwoman CLARKE. I thank all of our witnesses for their testimony here today and I will remind the subcommittee that we will each have 5 minutes to question the panel.

I now recognize myself for questions.

For Mr. Ley, the cyber attacks against the Oldsmar water treatment facility and the Colonial Pipeline earlier this year, coupled with on-going reports that our adversaries are using cyber tools to target critical infrastructure have renewed conversations about how to better defend our OT networks.

As employers gain a greater understanding of the gaps in their OT cybersecurity work force, it is clear that employees will need to be re-skilled or upskilled for these positions or receive additional trainings through continuing education programs.

What steps are necessary to facilitate access to the trainings and certifications required for these positions?

Mr. LEY. It is a great question, Chairman Clarke.

The issues lies deeper than the access. There is a lot of access to a lot of academic information training courses and so forth. Again, what seems to be—surprised most folks—and we have gone to many different organizations, energy companies, water treatment facilities, to your point, businesses, manufacturing companies, even municipalities, and when we talk to them they really don't even really know where to start with identifying the education that they need, what topics. I know that sounds very strange, but we have developed methodology, we have task analysis surveys, we use the NICE framework to ask questions on what

---

[30] H.R. 3138, "State and Local Cybersecurity Improvement Act." Retrieved from *https://www.congress.gov/bill/117th-congress/house-bill/3138/text.*

[31] H.R. 2980, "Cybersecurity Vulnerability Remediation Act." Retrieved from *https://www.congress.gov/bill/117th-congress/house-bill/2980/text.*

[32] H.R. 3223, "CISA Cyber Exercise Act." Retrieved from *https://www.congress.gov/bill/117th-congress/house-bill/3223.*

[33] S. 1097, "Federal Rotational Cyber Workforce Program Act of 2021." Retrieved from *https://www.congress.gov/bill/117th-congress/senate-bill/1097.*

[34] H.R. 3599—117th Congress (2021–2022): "Federal Rotational Cyber Workforce Program Act of 2021." July 2021. Retrieved from *https://www.congress.gov/bill/117th-congress/house-bill/3599.*

their folks do and where they touch cyber, IT, and OT. Obviously they need to know that to know where to send their folks and how to educate their work force and their organizations. Consistently—consistently, they don't have an idea.

So we developed a process and a tool set, not just ours but in conjunction with other businesses that already have some of these solutions out there, that can—entities, organizations can utilize, even Government agencies, to sit down first and start with identifying what are the educational needs of their individuals. You can't fix a vulnerability, you can't fix or mitigate a threat if your folks aren't even aware what they should know and how to know that there is a threat even targeted at——

Chairwoman CLARKE. Thank you, Mr. Ley. Let me move on. We have a short period of time, but we—to be continued.

Mr. Nolten, with support from additional discretionary funding from CISA, cyber.org recently launched a K–12 feeder program with Historically Black Colleges and Universities and Minority-Serving Institutions to encourage more minority students to seek cybersecurity degrees.

Please elaborate on how this program will work and the goals you have for it. With additional Federal support how would you be able to expand your efforts to reach more students of color?

Mr. NOLTEN. Great question, Chairwoman Clarke.

Cyber.org's HBCU feeder program and Minority-Serving Institution feeder program is key to diversifying the cybersecurity work force. Our work is ensuring that high schools who are feeding into HBCU programs have the availability of curriculum, professional development, technology, and resources to stand up a cyber lab or a cyber classroom in order to introduce students to cybersecurity careers.

K–12 education, as I mentioned in my testimony, is the formative years for ensuring that students have awareness of what they want to be when they grow up. If we ensure that our work is placed in Title 1 schools, in rural communities, we will begin diversifying the cyber work force by partnering with MSIs and HCBUs across the country.

Chairwoman CLARKE. Mr. Stier, a major challenge for Federal agencies has been retaining skilled cybersecurity professionals, yet agencies do not necessarily track the reasons behind the poor retention.

What should agencies like DHS and CISA do to better understand why cybersecurity employees choose to leave and what steps can agencies take to improve retention?

Mr. STIER. Great. Thank you so much for the question. I will give you at least three.

The first is, I mentioned in my testimony that exit interviews would be very helpful in understanding, so long as there was real-time turnaround of that information and it went to leadership. If it is collected and it doesn't got to leadership, it is not going to make a difference.

No. 2, we already have the Federal Employee Viewpoint Survey, which is how we create our places to work rankings. We have data on an annual basis that tells us what is really going on in every

organization in government. Leaders should be held accountable for those numbers, and that would make a very big difference.

The third and most important issue is that, again, leaders have to see that this is their job and responsibility and the most senior leadership in Government has to hold the people who work for them accountable to ensure that these numbers are good. If they prioritize it themselves, you will see change.

Chairwoman CLARKE. Mr. Stier, I think your screen froze. But I am out of time. We will circle back.

Let me now recognize the Ranking Member of cybersecurity, the gentleman from New York, Mr. Garbarino, for his questions.

Mr. GARBARINO. Thank you, Chairwoman. Thank you to all the witnesses again for being here today.

I want to start with Mr. Stier.

I really do appreciate some of the things you said in your testimony about concrete items that we need to change. You pretty much took my first question away from me, which is good, but I want to build on something because you talked—you specifically mentioned how we should hire—we should get interns and interns should be able to come right in after they—college interns and they can come right in after they have completed their internship. That is what a lot of—that is what law firms do with kids in law school, that is what bankers—I mean it works for the private sector, so I think it would be great at getting young people involved. Right now I think it takes almost possibly—getting a job at CISA a new hire can wait for a year. A college student coming out of college can't wait a year if they have got debt.

So, you know, what exactly—I mean is there a process there that you are thinking of? You know, what exactly should we do? How do we cut down on the year wait list?

Mr. STIER. Yes. So you are 100 percent right. I mean and the most obvious example of what needs to happen is our Federal Government needs to approach talent management as the best private-sector organizations do. The most obvious thing in any professional organization, it starts with its strategy. As we do at the Partnership for Public Service, we think our student internship program is our primary mechanism for identifying talent for entry jobs. That is not happening in the Federal Government right now. There are some rule changes that Congress could institute. They could make it easier to converge interns into full-time employees. Right now, if you are unpaid or if you are hired by a third party, even one that gets diverse talent, that is much more difficult to actually convert in. So those are real rule changes that would make a difference.

But fundamentally, I think the issue is really having leaders inside Government, the agency Secretaries, the different component heads, as well as the career leaders, understanding it is their responsibility and having clear metrics about what the expectation is. It is not working right now. It has gone the wrong direction. So we have seen fewer and fewer young people in Government today. It is not because of lack of interest. It is not because of lack of interest. That is relevant, but that is not the primary issue.

So it would be, No. 1, hold leaders accountable. No. 2, make a few rule changes that would make it easier to convert interns into

full-time employees. No. 3, make sure that there is real budget for this. That includes making sure that the interns are actually paid. Then the other issue, clearly in cyber in many instances, is security clearances. One of the things that can be done is ensuring that the security clearance process is completed while interns are students. There are different agencies that do this better. So we should be drafting on the approaches that the agencies that are best in class are using for all of Government.

Mr. GARBARINO. I appreciate that. That is a great answer. Does anybody—any of the other witnesses want to jump on anything additionally we need to do?

Mr. COULSON. I would just like to interject. Internship is one process, but I think there is a huge opportunity here for apprenticeship. To have people earn while they learn, but also increases velocity because students are able to gain experience while they are in their job, while they are receiving their education. It also tightens the partnership with educational institutions to build the work force you need as opposed to well, here is somebody we graduate, I hope it worked out. It is a much more integrative approach.

So I would suggest that that would be something that be explored and I would be glad to talk to you further about this as we are about to in the CAE community pilot a major apprenticeship program in cyber directed at Government.

Mr. GARBARINO. Now, your apprenticeship, would you—the apprenticeships would be with the Government or with private companies and the people could transfer into the—I mean how would—what is your—how are you doing this? What is the pilot program?

Mr. COULSON. Well, it is both. Because of the interest of time, it is complex to describe, but let me just say that I think that the apprenticeship model has been incredibly underused and there is a lot of energy coming out of other parts of the Government, and I would like to see that in the area of National security, because it allows us to mentor and produce and validate talent while they are in school and while they are working.

Mr. GARBARINO. I appreciate it, Mr. Coulson.

I hope we get a second round of questioning because I had a couple more, but I yield back.

Thank you, Chairwoman.

Chairwoman CLARKE. Mr. Ranking Member, should time permit I definitely support that.

Let me now recognize that—other Members for questions they may wish to ask our witnesses.

In accordance with the guidelines laid out by the Chairman and Ranking Member in their February 3 colloquy, I will recognize Members in order of seniority, alternating between the Majority and the Minority. Members are also reminded to unmute themselves when recognized for questioning.

Having said that, the Chair recognizes for 5 minutes the gentleman from Rhode Island, Mr. Langevin, for his questions at this time.

Mr. LANGEVIN. Thank you, Madam Chair. I want to thank our witnesses for their testimony today. Very insightful.

I will also mention, with respect to the Ranking Members' line of questioning on internships and apprenticeships, I applaud those

efforts. That is why I am also a big fan of the cyber core program, whereby students can apply at that program and if they are accepted tuition is covered for the junior and senior year. They will be able to—they get paid a stipend, about $32,000, and then they go into a cyber job at local, State, and Federal Government for 2 years after that.

Let me get to another—my line of questioning.

Mr. Ley, I am very interested in proving cybersecurity training among our operational technology work force. The Chair, Madam Chairman, had brought up this during her line of questioning. So that is where we are simultaneously further behind the curve and where most damage can be done.

So our National cyber director, Chris Inglis, often talks about cybersecurity education having three tiers, the many, the some, and the few. So the many are the people who use technology in their every day lives, which is to say almost everyone. Mr. Nolten has done an admirable job describing expanding K–12 education for everyone. The few are the cybersecurity professionals who have cyber as part of their job titles. The kind of folks Dr. Coulson's programs churn out. But I want to focus on the "some", the people who in the IT world are the software developers or network architects.

So these are the people who need a much more nuanced view of cybersecurity than most, but for whom it remains secondary to their main job function. In the OT space, these are the maintainers, the installers, the operators of industrial control systems.

So I continue to be concerned that while training for these occupations includes an incredible emphasis on a safety culture, cyber risks have barely penetrated.

So, Mr. Ley, in your view how can we better incorporate cybersecurity into the training for OT professionals who do not focus on cyber?

Mr. LEY. Thank you, sir. Great question.

We have a lot of the information. Obviously our training courses cover a lot. Unfortunately, expanding that information out to other platforms to offer that, businesses out there, the organizations, the local municipalities, can't necessarily afford some of the training that they actually need. Some of the training that we offer, working with CISA right now, looking at opportunities to take the curriculum we have, offer it to universities, colleges, other institutes, take the information we have, take the curriculum and let them offer the same curriculum and provide them support so that those businesses out there, the some, the nations out there, don't have to come here, they can go locally. Universities and colleges can start developing these offerings themselves. They know the businesses, they know the organizations, they know the specialties they need. A lot of academic institutes come to us and say we need this specialty. We can develop it and we push it out. That is the area we recommend really needs to be developed.

We started to explore that, but that would be where I would ask.

Mr. LANGEVIN. Thank you.

Let me get to another question for Mr. Stier. In your testimony you referenced the need to update pay and classification for the Federal work force. This is something that the Cyberspace Solarium Commission, on which I serve, has looked at closely. Madam

Chair, I ask unanimous consent that the Solarium Commission's white paper entitled "Growing a Stronger Federal Cyber Work Force" be inserted in the record.*

Mr. Stier, would you take it from the administration and Congress to get the—what would it take from the administration and Congress to get the civilian work force competitive with the private sector? Should the National cyber director chair this effort, which will necessarily involve several elements of the inter agency?

Mr. STIER. So, look, I think that it does make sense to have a coordinated response. I will note that one of the things that as legislators you need to pay great attention to is you actually put legislation in in 2014 to give authority to DHS on cyber pay. It is just getting rolled out right now in September. That is too long. You can't wait 7 years for this kind of action.

So one risk of creating the sort-of National or Federal-wide effort is that there will be a lot of talk and not a lot of action. So I would be looking to actually be setting up, you know, time tables about when things actually need to get done and clear metrics about what success looks like. But it begins with having an enterprise-wide, a Government-wide plan about what we need in the way of human capital and then what do we need to do to get it. A lot of it may be upskilling existing talent, it could be new talent. I see the clock has run, but I would be thinking about it in a strategic way to approach the problem.

Mr. LANGEVIN. Very good.

My time has expired. I thank you for the insights you have offered.

Madam Chair, I yield back.

Chairwoman CLARKE. The Chair now recognizes for 5 minutes the gentlewoman from Tennessee, Ms. Harshberger, for 5 minutes.

Ms. HARSHBERGER. Thank you, Madam Chair, and thank you witnesses for being here. This is to me a really exciting topic because we are so deficient in cybersecurity work force. From different meetings I have been in, you know, it would take a million people to fill some of the slots that we need, but to me that is unbelievably—that is ridiculous. We need people.

You know, when I go around my district, I make sure to tell every entity I can, every school system, anybody who will listen, encourage these young people to look at this field.

I guess one of my first questions is for Mr. Stier. You know, I am sure you are aware that DHS has yet to finish its development and roll out of the CTMS program. The main goal of this initiative is to cut the time it takes to hire these cybersecurity professionals. Really to redefine how the Government evaluates their skill set and their pay rates. You know, I was talking to someone at one of the think tanks and they are like, they can really ask whatever they want and we take them because there is such a need.

You know, the committee is concerned about how long it takes DHS to implement this program, which was authorized back in 2014. What is your perspective on how effective a tool this will be for the Department?

---

*The document has been retained in committee files and is available at *https://www.solarium.gov/public-communications/workforce-white-paper.*

I guess my other question is what recommendations do you have for DHS so we can meet those goals? I am doing all I can to tell people about a field that I think would be very interesting for even middle schoolers going on up to high school, before they ever get into that arena.

Mr. STIER. So, Congresswoman, I think you are—it is so important you are doing what you are doing because your voice really matters to encourage people too. I just see this as a field for themselves or something that, bluntly, should be part of whatever else they are doing. I think the direct answer to your question is that we really need more consistent long-term leadership on these issues.

You are 100 percent right, this has been crazy-slow in an area where slow is incredibly dangerous. The risk moves so fast that by the time you get to where you think you need to be, you are already behind the curve. I have heard, you know, folks in Government say we work real hard to catch up to the past. That is not where we need to be.

I think fundamentally the most important structural change that you could make is ensuring that we had consistent leadership on these management technology issues across administrations. So think of this way, the FBI director has a 10-year term, the comptroller general at GAO has a 15-year term. The reality is GAO is one of the best-run organizations in Government because you have a leader who knows that the work that they do around talent will actually pay off for himself.

I would suggest that you think about trying to ensure that there is cyber leadership that is consistent over the years. Again, I mentioned this earlier, that Secretary Granholm wants to see the CESER leadership actually be career. I would be thinking about that CISA as well. You have a really strong person there right now, but if the average tenure is 2 years, there is no way you are going to actually see significant progress. People inside are all going to be running toward the new leadership and very careful about not getting too far over their skis knowing that someone new is coming in and that becomes a real problem.

So that to me would be my No. 1 suggestion. There are other things I think you can do, but I will be quiet for now.

Ms. HARSHBERGER. Well, you know, it is almost like when you hear these experts talking and they are saying people can even use Google and look at traffic patterns in certain countries. I am like, that is unbelievable. Does it take a 4-year degree? How are you going to get these people interested to go into this field because the need is so critical?

To me, we would designate this need as critical infrastructure if I could, but we can't do that. If anybody wants to answer, do they need a 4-year degree? What kind of degree do they need to even enter this field?

Mr. COULSON. I would interject, we work a lot with community colleges, but I think there is a mantra here.

Career technical education especially—people have looked at it, well, that is vocational, that is, you know, welding and things. No, cyber fits there too. Often times in my work we have to let kids find out how smart they really are. That is usually education be-

comes a gateway drug, if you will. So if we can identify them and we have a program where we are looking at aptitude for cyber, not aptitude in terms of you can and you can't, but where do you fit? Then to identify them and come up with programs that nurture that talent all the way through. We could have kids coming out of high school that could work at the technician level. We have community colleges that are now even doing not only associate's degrees and certificates, but are also including bachelor's degrees.

I think academia has a reputation of being glacial, but I would suggest that that is not necessarily a fact in the cyber space.

Ms. HARSHBERGER. Well, Mr. Coulson, you are speaking my language.

My time is out and I thank you.

I yield back, Madam Chair.

Chairwoman CLARKE. The Chair now recognizes for 5 minutes the gentleman from New York, Mr. Torres.

Mr. TORRES. Thank you, Madam Chair.

Three years ago I came across a *New York Times* article with the following headline: "The Mad Dash to Find a Cybersecurity Workforce". The article was citing cybersecurity ventures, claims that by 2021 the cybersecurity work force would have 3.5 million vacancies. We are in 2021.

So I am curious to know has that projection come true? What is the extent of the shortages in the cybersecurity work force as of 2021? Anyone who has an answer to that question can feel free to answer.

Mr. COULSON. OK. Everybody has a prediction on that. That might be a global number, but within the United States right now, you know, best that I could find this morning was actually just over 500,000. That is in the compressed hiring that we are in right now. But the Solarium Commission report that Representative Langevin worked on, says something I think is overall answer to that question, and it is we have had reports, we have had predictions, we have had things for 20 years. What we need is action on it, because the problem has not been getting better, it has been getting worse.

Mr. TORRES. In order to—and I am in favor of action, I just want to understand the precise nature of the problem. So are these vacancies—to what extent are these vacancies coming from the public sector and the private sector? Do we know the breakdown? Do we know the number of vacancies that require a college education?

Mr. STIER. So I can speak—this is Max Stier at the Partnership—I can speak to the Federal Government. The answer is we really don't know what the real need is. This is my point about the importance of really doing a more thorough human capital plan for the Government in cyber and beyond. I think we need it in more than that.

I can't resist also saying that the gap is not simply in the actual technical talent, the gap in some ways is more profound in the fluency around these issues, in the leadership more broadly. You know, people who are not actually in jobs that are designated as technical positions fundamentally actually need to understand these issues in order to do their work appropriately.

I think if you are thinking about what the actual gap is, you ought to be examining that one as much as the actual work force.

Mr. TORRES. Is that a number—we need more cybersecurity generalists? Is that?

Mr. STIER. It is less that—I would say, for example, that if you are coming in as the Secretary of an agency in the Federal Government, if you are running a component, if you are a career senior executive running a large program, you have to be thinking about cyber issues and understanding what the implications are for your programmatic choices. That includes, you know, the talent needs. You will need to be able to address those problems. That is an information gap. You don't need a cyber professional in those positions, but you need people who are fluent and aware.

Mr. TORRES. I have a question for each member of the panel. What is the most successful cyber work force development initiative that you know of and that should be scaled up?

Mr. NOLTEN. I will jump in, Congressman, and mention that CETAP is proven to be a successful program in that we are introducing students to cybersecurity careers and degree opportunities at an early age, elementary and secondary.

When a student asks me what do you want to—or when I ask my students, what do you want to be when you grow up, at that very moment I am providing them a gateway into the opportunities that exist for them post-high school as well as post-graduate. Not every student is going to go to college and so what we want to ensure is that upon graduating high school we have students with industry-based certifications, that they are skilled to go walk into an organization and be employable immediately. Employability is the key and we want to see that CETAP be grown so that high school students who are going into any of the 17—16–17 critical infrastructures within DHS's structure, that those students have the ability and the knowledge to——

Mr. TORRES. Can I interject? What is your placement rate?

Mr. NOLTEN. I am sorry, sir?

Mr. TORRES. Your placement rate.

Mr. NOLTEN. So right now we see that high school students who are participating in CETAP's program, four times as many students are going into a cyber-based degree field within a 2-year and/or 4-year program.

Mr. TORRES. How many students have gone through your program?

Mr. NOLTEN. Over 3 million students have benefited from our program in all 50 States.

Mr. TORRES. Does the rest of the panel have any thoughts on what is the most successful existing cybersecurity work force initiative?

Mr. LEY. I would—I am sorry.

Mr. COULSON. Please go ahead.

Mr. LEY. I would like to suggest there is a program that is not even funded and even an initiative right now, and it is to match. What we find in our research is that the students coming out of degree programs, even out of high school, and the hiring at these organizations, businesses, Government entities, there is not a defined mechanism to really place the most talented individuals in

the jobs where they can be the most successful. There is nothing based on the old hiring process of resumes and interviews is what is taking place. We continue to hear from businesses, Government entities, well, we hired the most—we thought was the best person and it takes us 18 months to 2 years to get them trained up to be useful. Why is that? Because there is not a mechanism. You identified the mechanism, but there is no funded program to actually implement that to say nice KSATs, hiring job applications has the same KSATs, we can see what the students have, what skills they have and match them to the job and the people can hire the right people the first time instead of the second and third time.

That is an issue that should be out there.

Mr. TORRES. My time expired, so I am going to——

Chairwoman CLARKE. Thank you very much, Mr. Torres.

The Chair now recognizes for 5 minutes the gentleman from Georgia, Mr. Clyde.

Mr. CLYDE. Thank you very much, Madam Chair. I appreciate this very important hearing.

One of my concerns is the dependence that we have on the H–1B visa program, or the student visa program. Oftentimes we see our universities and businesses invest in people that we bring in from overseas and we teach them cyber and they take up the opportunities that we have in this country and they learn all sorts of great things and then they take their talents and they go back home to their home countries.

So I see that as not being a great return on investment and we are losing out on the opportunity to develop Americans who can fill those jobs.

So I guess my question—and I would like to start with Dr. Coulson—so how can we best encourage the home-grown talent so we don't have to depend on the H–1B talent that at some point is going to go back to their home country and we are going to lose that opportunity and what has been invested in those people.

Now, I understand that those people might actually, you know, bring something to us as well, but still, you know, they are not American citizens. You know, they are not going to stay here. They are going to go home and take that talent and everything they learned with them.

So how do we do that? How do we best encourage home-grown talent?

Mr. COULSON. So two-thirds of Ph.D.s in this country are non-domestic. That is a crisis in itself. There is a number of programs that I could inform you of after, but in the interest of time.

The research program that we just started is really looking at, all right, how do we home grow talent. It doesn't have to be all from our one university. Again, I will go to my mantra, kids sometimes don't know how smart they are.

Mr. CLYDE. Right.

Mr. COULSON. So the program we created now with 38 universities, working with technical directors on actual problems is meant to reach into the undergraduate level and start teaching them the science of research so that we can pipeline these and grow our domestic talent and also develop an affinity for the real challenges that Government is doing.

In the Centers of Academic Excellence Community I think that is a great example of something we are doing to tackle that one issue, which is very significant for the future of technical leadership in the United States.

Mr. CLYDE. Well, thank you. I appreciate that.

You know, as part of the Department of Homeland Security subcommittee, you know, one of the greatest threats we have is ransomware from the outside. So I think one of the greatest defenses we have is home-grown talent that can defend against that.

So does any other of the witnesses, would you like to add anything, Mr. Nolten or Mr. Ley or Mr. Stier, to that?

Mr. LEY. I would also bring back attention to what Tony brought up earlier about apprenticeship programs.

Mr. CLYDE. Right.

Mr. LEY. It is a way to bring the—start the folks out in a company and let them learn and their actual reason—to understand why they are learning, because they are working for that business. Apprenticeship programs are huge and a key. We really need to focus on that. Right now there really is not—in the Department of Labor or Department of Commence there is really not a defined apprenticeship for cyber-related skills. There is a reason plumbers and electricians have apprenticeship programs, because you can't get all the hands-on training just sitting in a classroom. Apprenticeships bring that and they are huge.

Mr. NOLTEN. Congressman, if I may add——

Mr. CLYDE. Thank you very much. That is an excellent insight. Go ahead, please, Mr. Nolten.

Mr. NOLTEN. Congressman, if I may add one statement here. Research has shown that a child begins to form what they want to be when they grow up around the middle school level. That is sixth, seventh, and eighth grade. If we look at other countries around the world and see where their dollars are being invested, it is in K–12 education.

So in order to begin solving this pipeline issue that we have, we have to focus on ensuring that we have students who are skilled and knowledgeable about the opportunities that exist in cybersecurity.

Mr. CLYDE. All right. I think that. Thank you.

I appreciate that and unless anyone else has a comment, then, Madam Chair, I yield back. I think that is great information though.

Chairwoman CLARKE. Thank you, Congressman.

The Chair now recognizes for 5 minutes, the gentlewoman from New York, Ms. Rice.

Ms. RICE. Thank you, Madam Chair.

I would like to continue talking a little bit more about community colleges. I think we all agree that they play an incredibly important role in connecting students with an affordable higher education. In my district, Nassau Community College, which is a Minority-Serving Institution, has a cybersecurity certificate program designed for students who intend to go onto pursue a 4-year cybersecurity degree.

Dr. Coulson, do existing Federal programs adequately support programs like the one I just described at Nassau Community Col-

lege? What if any additional resources may community colleges, particularly minority-serving institutions, need to assist them in building, growing, and diversifying the cybersecurity work force programs?

Mr. COULSON. Well, the Centers of Academic Excellence program has over 150 community colleges. We have set up a National articulation database. That was with Moraine Valley Community College. That is some great work with the National Science Foundation's advanced technology education program with Whatcom Community College and Cal State San Bernardino were working through the community college network to see what is it that employers want, but also how can we diversify talent on so many ways? We have something called the Cyber Education Diversity Initiative, which focuses on Minority-Serving Institutions, but also we have program for the deaf and the hard of hearing, Wounded Warriors, neuro-diverse communities, and so on. I think the community colleges play a pivotal role. A lot of times it is in the area traditionally seen as re-skilling, but I would say that it is also upskilling.

So I think that community colleges in general are really an economic engine and especially for opportunity for many people. The issue that we have in the Centers of Academic Excellence in terms of funding is everything is one-time funding, one-time grant related through a number of agencies. I would really like to see the Department of Homeland Security invest in this program with sustained funding so that we aren't doing hand-to mouth, but we could attack this problem strategically.

Ms. RICE. That is actually a really good point and I think that we should take that advice about the funding. I think that is critical. I agree with you.

You know, I think there is also a misconception that all cybersecurity jobs require an advanced degree. But cyber.org's website explains in the—its cyber career profiles that there are a number of good-paying cybersecurity careers that don't necessarily require a degree at all.

Mr. Nolten, you know, we are talking about K–12 and I know that you have experience working with K–12 educators, what more can be done to increase awareness of the full range of cybersecurity career options that are available to young people? I think it is really important—I think the Federal Government needs to support high schools that want to implement career and technical education programs around cybersecurity that are designed to, you know, send students into the work force right after graduation.

But, Mr. Nolten, if you could just talk a little bit more about how can we increase awareness? I think that, you know, if kids knew what was out there—you know, I forget who—I think you said that—talked about that critical time period of sixth, seventh, eighth grade where kids are beginning to make kind-of career choices. If they are not hearing about it in school and they don't know what the potential is, then they are missing that opportunity.

Mr. NOLTEN. Congresswoman Rice, I mean that is a great question and it is a great awareness that we must take.

One simple example, Sally has two apples at the house, she has five friends coming over, how many apples does Sally need to go

out and buy. This is a simple subtraction problem that many of our educators are using. My encouragement to K–12 educators is don't use apples, use gigabytes. Sally has a computer at the house, it has two gigabytes of memory, she has a really cool program she wants to run that requires five, how many gigabytes does Sally need to add? By changing the context of what we are teaching inside the classroom, we are able to introduce these students and place seeds of opportunity in our minds of our students. This very work, this very structure, we allow students to explore career opportunities that they have no idea about, their mom or dad or guardians had no experience in. This effort and this movement must be scaled. We must ensure that teachers have the confidence, the ability, and the resources from a funding standpoint to be able to teach cybersecurity and to change those apples to gigabytes.

Ms. RICE. Well, thank you all so much. I think this has been a great discussion.

Madam Chair, I yield back. Thank you.

Chairwoman CLARKE. Thank you, Congresswoman.

The Chair recognizes for 5 minutes the gentleman from Kansas, Mr. LaTurner.

Mr. LATURNER. Thank you, Madam Chairwoman.

Mr. Stier, let me start with you. There is a seemingly endless supply of cyber work force related legislative proposals. But I am concerned that often times Congress focuses on the shiny new bills instead of conducting the necessary oversight to ensure the prior bills have been properly enacted.

Where should the committee be focusing when it comes to oversight over enacted lines of effort?

Mr. STIER. So thank you for such a wonderful question. I agree with you that often times we see problems Congress legislates and then done, move on to the next thing. The reality is, in my view, legislation is the starter's pistol, it is actually not the race. Your oversight function is profoundly important.

So one of the recommendations I made in my testimony was that you actually make this an annual testimony, or rather an annual hearing. I love the example that was given earlier about the need for long-term money, because there is no way to plan on these programs if you don't have multi-year funding. It is the same here, if you let agencies know that this is not about giving them an authority and then walking away, but rather that you have actually a plan, you intend to be able to have oversight on an annual basis with a set of metrics, performance metrics, that you build into your thinking. That may change over time. I think that will change the incentives for agencies and the likelihood that you actually see more progress from the investments that you are making.

So I would think about this, again as you suggest, not as a, you know, legislate and walk on, but rather what are our goals, you know, what is our current thinking about the tools we need right now. How will we know whether or not we have been successful. Then come back to it in a regular way with notice to agencies that this is about to happen. I think you would see in different outcomes. Not easy outcomes, because, bluntly, these are tough problems and they are problems that are changing.

Mr. LATURNER. I appreciate that.

This question is for all of you and it is a really broad one. With so much focus in recent years about expanding cyber educational opportunities, do we feel like we are at the point that we are starting to close the gap, are we making a dent?

Mr. LEY. I will just say from my perspective, from a lab perspective, from testing control systems and looking at and providing courses to folks, I think we are making a dent. Some of the issues are very systemic and I think are just not known, even to panel members. We talk about the tools that connect the high school, get them excited there. There's lot of progress. I have 23 interns from colleges and universities around my State and other universities around the Nation and I ask them, if you are in a degree program, a cyber-related degree program, why? What are you going to do with it? They don't know. There really is not a mechanism—there are mechanisms out there, we are not connecting them to what jobs they need to go to.

So as far as degrees and topics we are teaching, yes, I think we are making a dent, I think we are offering the right curriculum and I think it will ever be expanding. It is not going to change. But we have got to connect the students who have moved on and are excited, think they know what to do, they get to that next level and they are—where are the tools, where are the things I can go to look to what is next for me. They are not being exposed to those.

Mr. LATURNER. I appreciate that.

Yes, Mr. Coulson, go ahead.

Mr. COULSON. So 6 years ago when we started the Centers of Academic Excellence Community, we were about 15,000 students. We now have over 100,000. A lot of that has to do with a long-term vision reaching into the K–12 space, seeing the dividends of programs like cyber.org, the GenCyber camp program, and others that are stimulating interest. We are starting to see that bubble up. But it is a long-haul game. I think that is a real message here.

As you said earlier, shiny object funding is not going to solve this problem.

Mr. LATURNER. Very good.

Mr. Stier, I saw you have your hand up.

Mr. STIER. So, yes. I think just to—there are a lot of people working really hard on these issues and we are making, in absolute terms, progress. But what I would say is that fundamentally this is about dealing with problems that are in the real world and against the problem set that we face, my view is we are losing ground not gaining it, certainly in the arena that I can see.

Mr. LATURNER. Wow. I want to hear your perspective.

Go ahead, Mr. Nolten.

Mr. NOLTEN. Congressman, two quick stats. CETAP's impact is well over 3 million. While that may be an exciting number to many, the denominator there is 52 million. Our work has just begun.

Mr. LATURNER. Thank you so much.

Madam Chairwoman, my time has expired. I yield back.

Chairwoman CLARKE. Thank you, Congressman.

For colleagues who may be interested, I am going to enter into a second round of questioning. There are a few questions that I have remaining. For anyone else on the subcommittee who also

may have additional questions, you will have an opportunity at this time.

Dr. Coulson, a major part of addressing our cyber work force shortage must include re-skilling workers for cybersecurity jobs. I think certainly in the midst of this pandemic where we are hearing about the great resignation, there may be an opportunity if we open our eyes wide enough or open the aperture so that we are looking at some of our employees who may not be returning to some of the professions that they were once in.

How are universities and community colleges currently working to include nontraditional students already in the work force or in their programs? What barriers exist for participation and what can we do to expand access?

Mr. COULSON. Well, that is excellent. This is something I am so excited that you asked me, to be quite honest. Re-skilling is absolutely necessary, it is absolutely important. I think the academic community has looked at cyber and said, look, we need all hands on deck. How do we get somebody with an existing degree or maybe had a different life before, how do we see where they fit in cyber, which is such a broad field.

We ran a pilot program with the National Science Foundation that provided scholarships for veterans and re-skilling workers through the community college program to get them into the cyber work force. We wanted to see what was making them tick.

But more than that, on a broader spectrum, we are seeing programs that are emerging in our Centers of Academic Excellence and we are incentivizing them not only in on-line learning, but in other ways that fit around schedules so that somebody could still actually work in their job but look toward a new career and make accommodations for different age groups and people who are differently abled.

There are so many programs there and I would love to have a longer discussion on it, but we—I will say this, we are working in that area because it is so very important and universities and community colleges are expanding capacity as much as possible, marketing. Actually, next month we are running a National virtual career fair for cybersecurity students and trying to link them with employers, but also try and stimulate interest in re-skilling.

Chairwoman CLARKE. Got caught out there for a moment.

This is to the panel. What should the Federal Government's role be in facilitating apprenticeship programs in the private sector? If you have given any consideration to that.

Mr. COULSON. I think Mr. Stier said earlier, what are the standards for a cybersecurity discipline. So we actually just started a project with the American Council on Education to try and help set those standards, and we are going to work with the Department of Labor to see if we can get at least the first of what we consider many different disciplines within cyber, because obviously this critical infrastructure and so on.

One of the areas that I think the Federal Government could really help us in, especially in the Department of Labor, is velocity. To get the apprenticeship programs moving is such a laborious technical process that many of our industry partners have said, I don't understand this and they are ready to walk away. I would really

like to, you know, work or maybe put together subcommittee on how we could fix that problem and increase velocity. Because apprenticeship is very foreign in the United States but it is such a key—has such key potential to solving this problem.

Chairwoman CLARKE. Very well.

I wanted to do a deeper dive with you, Mr. Stier, about how agencies can improve retention. We know that, you know, there is great demand for the limited talent that exists. We are constantly hearing of private sector poaching from the public sector. Could you give us a little bit more depth to what we can do in the retention space?

Mr. STIER. Absolutely. It begins to have real-time data on what is actually happening and have leaders that are held accountable for that data. Otherwise, you know, there are a lot of things you can do, but you don't know if you are doing the most important things.

You know, what we see in the work that we do is, No. 1, especially young talent, they want to feel like they are being invested in. I will note that there is a really—in my view, a big difference in the way by and large the uniformed services are treated versus the civilian services. In the military by and large they see their talent as an asset. Oftentimes the talent inside the Federal Government, the civilian talent, is treated as if it is a cost. We need to see I think way more investment in the people in the knowledge that they are getting, in the responsibility that they are getting, and also in the management that they are getting. If you did that, I am quite confident that you would see a lot higher retention numbers.

If you look at our best places to work rankings, the No. 1 issue for why people are actually leaving is their perceptions of their leadership, from the first line supervisor to the more senior people in the organization, and it is not good. It is, you know, 10+ points below what you would see in the private sector. They're purpose-driven, they want to be there, but if you give them bad management they are not going to say.

So that to me would be the most important thing to do, is improve the management, hold them accountable, provide real investment in their growth and responsibility. The Government has the best value proposition around. You can make a difference in the world, which most young talent really care a lot about.

Chairwoman CLARKE. Very well. Thank you.

My time has run out.

I now recognize the Ranking Member of the subcommittee, the gentleman from New York, Mr. Garbarino, for any additional questions he may have.

Mr. GARBARINO. Thank you, Chairwoman. I do have at least one more question.

Mr. Stier, we will start with you. The Cyber Corps Scholarship for Service program, run by the National Science Foundation, has been a great program to encourage students to enter public service. I understand that to date nearly 3,500 students have taken advantage of the program.

What more can we do to increase participation in this program? Or maybe not—and if not, it is not increased participation in this

program, what is the difference—is this program better or could we maybe start some sort of cyber university, similar to one of the other—like the Naval Academy or the Merchant Marine Academy? You know, the Merchant Marine Academy was started in 1943 because of shortage in merchant marines. We have a shortage in people that need to go into the Government cyber work force.

Is this something that we should be looking at, or should we just stick with training them at outside colleges and hope they come to work for us?

Mr. STIER. Sure. So, Congressman, I think this is a fantastic question. I come back to the military model, and you used it, which is you can think about the academies versus the ROTC. In my view it is much more cost-effective to make further investment in an ROTC model rather than the bricks and mortars of a new institution. It is not simply that it is more cost-effective, but it is also in my view more—you will have higher leverage. If you leverage off of the, you know, Government-wide—you know, we have best in class higher education in this country and if you create more scholarship opportunities for service in Government, you will—it will be, again, a cheaper way of getting great talent and it will be integrated against the whole of society, because you also want to make sure that people who are coming into Government represent the entire—geographically, racially, gender, all those things.

So my counsel would be to, you know, further invest in programs that are more likely ROTC than it is to try to create a new entity focused on a specific area like cyber.

I think you will find immediate return because you don't—it takes a long time to create an institution and we don't have that time. I think you will have better pay-off.

I will say that we can undoubtedly do better in the way we use that talent. The Chair's questions around retention should be applied here with the folks that—because, yes, they may have a service requirement, but you really want to have a program that keeps them well long after that service requirement has ended.

Then there are programs like what we have, the Cyber Talent Initiative, where we are partnering with the private sector, with MasterCard and Microsoft and Workday. They are actually supporting bringing talent into Government knowing that talent might also come to them.

So there are a lot of novel ways of trying to drive talent into the sector and into Government.

Mr. GARBARINO. I appreciate it, Mr. Stier.

Any of the other witnesses want to add on or have any thought on the question?

Mr. COULSON. Well, actually I am a scholarship for service institution. I would say that that was one of the keys that built capacity within my institution to create such great cyber talent. But there are other programs, like the Department of Defense Cybersecurity Scholarship Program that acts like an NFL draft, if you will, where the best talent gets submitted and they can pick and choose.

I think Mr. Stier brings up a very important point, and that is if we built bricks and mortar, it takes a long time, but also it closes the number of dimensions. I think a cyber university concentrating on one skill set is great, but that is not what cyber is about. Cyber

is so much broader and you need innovation from all sectors. As I like to say, innovate locally, deploy Nationally.

I think that is where the scholarship for service, and like Mr. Stier said, like an ROTC type of approach works probably more effectively and gives the taxpayer more bang for the buck.

Mr. GARBARINO. I appreciate that. Thank you very much.

Madam Chairwoman, I yield back.

Chairwoman CLARKE. Well, with that, I thank our witnesses for their very valuable testimony here today and my colleagues and Members for their questions.

The Members of the subcommittee may have additional questions for the witnesses and we ask that you respond expeditiously in writing to those questions.

Without objection, the committee record shall be open for 10 days.

Hearing no further business, the subcommittee stands adjourned. Thank you, everyone.

[Whereupon, at 11:32 p.m., the subcommittee was adjourned.]

APPENDIX

STATEMENT OF BITWISE INDUSTRIES

JULY 29, 2021

Chairwoman Clarke, Ranking Member Garbarino, and Members of the subcommittee: Bitwise Industries is grateful for the opportunity to submit this testimony in connection with the subcommittee's exploration of the need for and development of cybersecurity professionals.

Since 2013, Bitwise Industries, a female- and minority-led technology company headquartered in Fresno, CA, has been training underserved people from undervalued places for jobs in the digital economy. Our workforce training programs have prepared over 5,000 student workers, more than half of whom are women and/or people of color, for high-growth, high-wage jobs in the technology industry. Many of these individuals have gone from making under $21K/year to well over $61K/year. Following the program, 80 percent are employed in tech jobs resulting in $295 million of aggregate wages. In addition to outside employment, the technology consulting side of our business hires many of these students, proving it is possible to build stellar technology in unexpected places with diverse, nontraditional talent.

The key to our success is our apprenticeship model, which unlocks potential by coupling paid, experiential technical training with access and referral to essential services that address/remove barriers caused by poverty and bias. Our apprenticeship program is expanding to include a cybersecurity track for which we will seek Registered Apprenticeship designation. We employ a holistic and personalized approach to recruiting talent from underserved communities and building a nurturing community around them so that we can ensure that individuals have what they need to learn and thrive, including first and foremost, a sense of belonging. Their success then ignites and transforms the regional economies of the cities in which Bitwise Industries serves. Since launching in Fresno, we have built similar ecosystems in the California cities of Merced, Bakersfield, and Oakland, and recently announced our expansion into Toledo, OH. The next set of cities at the top of our expansion priority list includes Buffalo, NY and Birmingham, AL.

As you consider measures that Congress can take to facilitate the growth of an inclusive and skilled cybersecurity workforce, we urge you to examine with a critical eye barriers to the employment of marginalized people who have been persistently underrepresented in critically important professions such as this. Careers in cybersecurity are not only essential to the future prosperity and safety of our Nation, but also hold promise as a means of securing economic stability for many. These are jobs with salaries that ripple throughout overlooked communities if they are available to the full range of people who are qualified for and desire them.

UNDERREPRESENTATION IN THE CYBERSECURITY AND TECH FIELDS HURTS THE QUALITY AND QUANTITY OF RESULTING WORK

In 2021, evidence of the systemic underrepresentation and inequitable position of marginalized people in tech jobs requiring fluency in coding and networking exists anywhere one looks. According to Bureau of Labor Statistics data, as of 2020, just 9.1 percent of Americans employed in computer and mathematical occupations were Black, in a National workforce that is more than 12 percent Black. For Latinx workers just 8.4 percent are working in STEM fields, compared to 17.6 of all workers. Moreover, Black and Latinx workers constituted smaller percentages of the information security workforce than of all workers, and women were particularly absent from the cybersecurity field, accounting for just 11.4 percent of its employees, but nearly 47 percent of the entire workforce.

The relative inclusion of Black and Latinx workers and members of other underrepresented groups has declined since the publication of a 2017 report for the Center for Cyber Safety and Education, (ISC)², and the International Consortium of Mi-

nority Cybersecurity Professionals (ICMCP). The report found that while minority representation in cybersecurity professions was roughly consistent with comparable representation in the National workforce, other indicators of inequity abounded. People of color in leadership roles tended to be more highly educated than their white non-Hispanic counterparts, for example, but employees of color were disproportionately concentrated in non-management positions. In addition, both men and women of color working in cybersecurity reported lower average salaries than white counterparts, and workers of color were less likely to have received salary increases during the most recent year than white workers.

The effectiveness of our increasingly important efforts to secure information and operations that rely on connectivity are hindered by the disproportionate demographic characteristics of the cybersecurity workforce. As a recent paper from the Institute for Critical Infrastructure Technology observed, "Security teams that bring diversity of thought and perspective to the decision-making process are best equipped to navigate [the] complex ecosystem of players, technologies, and cultures" that must be taken into account in shaping cybersecurity solutions.

Experiential studies have confirmed that characteristics including age, income, gender, ethnicity, and cultural affinity affect participants' perceptions of information security risks in consistent ways; similarly, in other work-oriented contexts, researchers have found that teams whose members come from different walks of life excel at innovation and problem-solving because they benefit from the inclusion of a wide range of viewpoints.

The Nation's cybersecurity workforce would do its best possible work if it reflected our country's unique strength—the vast variety of cultures and experiences that shape us as individuals. Workplace leadership experts David Rock and Heidi Grant astutely pointed out in their Harvard Business Review article that collaboration across cultures "challenge[s] your brain to overcome its stale ways of thinking and sharpen its performance."

Government also risks squandering an opportunity to advance equity in access to programming and resources by failing to take transformative action to ensure that talented people from underserved communities find their place in the tech industry and in the short-staffed cybersecurity field in particular. When only a homogenous group of people who have historically been able to enter a system are charged with shaping it for the future, the weaknesses of the system are virtually guaranteed to be replicated consciously or unconsciously. Thus, if the Federal Government hires only people with advanced degrees or other qualifications that are expensive to obtain to be its recruiters, build its presence on-line, and protect IT networks, their work will naturally serve the needs and interests of others like them, and will fail to democratize entry. It is unsurprising that it has proven to be a persistent challenge for an institution whose workforce largely consists of individuals who are not underserved to design programs to effectively reach, serve, and protect its most marginalized constituents, since, for example, people designing websites for the Emergency Broadband Benefit or rental payment assistance programs are likely not to have had any personal experience using these resources. It is imperative that the Federal Government enlist more people, companies, and communities, including contractors and consultants, that historically have been excluded and that have themselves experienced the challenges it seeks to address so it can develop technical solutions for all Americans.

APPRENTICESHIPS UNLEASH PREVIOUSLY UNTAPPED TECH TALENT

Since our inception in 2013, Bitwise Industries has been preparing underestimated people for success in tech careers by offering flexible short-term pre-apprenticeship programs, paid apprenticeships, and holistic support for the people in whom we invest. Our experience with the thousands of individuals who have entered our training programs over the past 8 years has affirmed our conviction that apprenticeships are a critical, and as-yet underutilized, pathway into the tech workforce for members of underrepresented communities with the requisite talent and commitment to thrive.

Our apprenticeship model works for people who would not otherwise obtain the necessary knowledge and experience to enter this field because it eliminates the many practical and psychological barriers that reinforce systemic exclusion.

Perhaps most important is the fact that our trainees don't need to take on any debt to advance their careers. Pre-apprentices who need financial assistance receive scholarships and are able to work jobs around class schedules, and our apprentices earn a living wage with benefits while they are learning and building portfolios of work on the job. For each one of these people, our staff coordinates complementary services—from child care, to transportation, to access to hardware and a broadband

connection—that ensure that trainees have the time and mental energy to devote to developing their skills. We also value community and belonging, and we work hard to make sure that students and apprentices feel welcomed in our spaces and interact with peers with whom they identify when they come to a class or work team.

Graduates of Bitwise Industries' apprenticeships do not necessarily have resumes that resemble those of a typical tech or cybersecurity work team, but they are capable and talented, and they bring the kind of diverse perspective to their work from which the Federal Government's cybersecurity efforts would greatly benefit. A typical student or apprentice in one of our programs has obtained a high school diploma or GED but has not earned any tertiary degree or professional certificate; many of our trainees have come to us from employment in restaurants, retail, manufacturing, and farming. These individuals have repeatedly and consistently proven that, with the right environment and support, they can obtain in-demand skills and thrive in information technology jobs. Nearly all of our apprenticeship graduates, and four-fifths of those who have taken classes with us, remain in tech-oriented jobs today, and by their third year on the job, these people have secured average salaries of $81,000 per year. Bitwise Industries' tech consulting business has hired many of those who've completed apprenticeships through our program, so we can attest from personal experience to the acumen of our trainees in designing and building solutions for a wide variety of clients in industries ranging from agriculture to entertainment to finance and banking.

In addition to possessing requisite technical skill and collaborative ability, people who have trained for careers in information technology in Bitwise Industries' apprenticeships rather than through college-based academic programs are representative of the underestimated communities in that we serve, and comprised of people groups who have historically faced discrimination in the workplace and exclusion from the lucrative information technology field. We intentionally install our full ecosystem in cities whose populations are diverse in terms of race, ethnicity, national origin, educational attainment, involvement with the criminal justice system, family structure, and other circumstances, and we focus outreach and recruitment efforts in the most underserved and economically undervalued neighborhoods. As a result, about two-thirds of all of our students and apprentices have been people who identified as Black or Latinx. Women have easily outnumbered men in our classes and apprenticeship cohorts, and more than 40 percent of our people are LGBTQIA+ and non-binary. In addition, nearly half of our trainees have been undocumented individuals and people who are first-generation Americans, and many have belonged to groups recognized as encountering particular barriers to employment, such as people with criminal convictions.

HIRING STANDARDS AND PRACTICES MUST EVOLVE TO ACHIEVE INCLUSION AND FILL OPENINGS IN THE CYBERSECURITY WORKFORCE

As the capacity of Bitwise Industries' apprenticeship program expands and the success of our model inspires more providers to offer apprenticeship-style training for information technology fields, the pool of talent available to fill cybersecurity positions will grow and better reflect the full spectrum of Americans' characteristics and experiences. At the same time pathways into desirable jobs will need to adapt to recognize and take advantage of the ability that apprenticed workers possess.

Too often, the prerequisites to access opportunities in Government employment are mired in obsolete tradition, and designed to exclude or to achieve ends that are at odds with equity.

We urge Members of this subcommittee to push and mandate Federal hiring managers to reconsider credential and application requirements for cybersecurity and other tech jobs, and to eliminate or amend them wherever possible to open the door to a wider swath of the underserved population. For example, though degrees, certifications, and related job experience are typical barriers to entry into cybersecurity jobs, the Bureau of Labor Statistics has identified as the skills most critical to these roles attributes—problem-solving skills, ingenuity, attention to detail, and analytical skill in assessing computer systems and networks—that people can attain and develop just as well through practical training. Moreover, obtaining Federal Government employment usually demands not just that candidates have secured the requisite skill in the manner least accessible to marginalized individuals, but also that applicants possess the patience, networks, and background knowledge necessary to reconstruct their resumes and describe their experience in an idiosyncratic format. Instead of earning certificates and constructing narratives about their ability to do the work, Bitwise Industries' students and apprentices build portfolios of projects that showcase their work and allow prospective employers to see their skills. The

Federal Government's human resources systems should allow for multiple methods of demonstrating technical ability to ensure that people of all backgrounds can, and actually do choose to, compete for employment.

We note that President Biden's recent Executive Order on advancing diversity, equity, inclusion, and accessibility in the Federal Government instructs agencies to build pipelines into Government employment by deepening partnerships with colleges and universities that serve students of color and women. While these institutions are an important source of talent, their capacity is limited, and members of underserved communities continue to have less logistical and financial ability to pursue degrees than counterparts. To transform the face of the Federal workforce, the Government must look beyond its usual horizons and open jobs to—and direct recruitment efforts at—people like Bitwise Industries' students and apprentices, who have gained valuable knowledge and skills through nontraditional paths.

Thank you for your consideration of this testimony and your commitment to leveraging American workers' ambition and creativity to strengthen safety on-line and protect against attacks on the electronic resources and services on which we rely.